FortiSwitchOS Administration Guide

Standalone Mode

Version 3.6.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Friday, July 7, 2017

FortiSwitchOS-3.6.0 Administration Guide Standalone Mode

Change Log

Date	Change Description
July 7, 2017	Initial release.

TABLE OF CONTENTS

Introduction

This guide provides information about configuring a FortiSwitch unit in standalone mode. In standalone mode, you manage the FortiSwitch by connecting directly to the unit, either using the web-based manager (also known as the GUI) or the CLI.

If you will be managing your FortiSwitch using a FortiGate unit, please see the following guide: Managing a FortiSwitch with a FortiGate.

Supported Models

This guide is for all FortiSwitch models that are supported by FortiSwitchOS, which includes all of the D-series models.

What's New in Release 3.6.0

Release 3.6.0 provides the following new features:

- MCLAG (Multi-Chassis Link Aggregation)
- Dynamic Layer-3 protocols (OSPF, RIP, VRRP) (This features requires the advanced features license.)
- Route-map support
- Firmware Image Rotation (Dual firmware image support)
- TDR (Time-Domain Reflectometer) /cable diagnostics support
- Per-VLAN MAC learning limit
- Sticky MAC on switch interfaces
- PoE modes support: First Come, First Served or Priority Based (PoE models)
- ACL: Egress Mask Action support
- Monitor System Temperature (Threshold configuration, SNMP trap support)
- 'forced-untagged' or 'force-tagged' setting on switch interfaces
- Selective Packet Sampling to CPU (A useful diagnostic tool)
- Add CLI to show extended port statistics
- CLI display progress (%) during firmware upgrade

Refer to the feature matrix below for details about the features supported on each FortiSwitch model.

Feature Matrix: Release 3.6

The following table lists the switch features in Release 3.6 that are supported on each series of switch models. All features are available in Release 3.6.0, unless otherwise stated.

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
Link Aggregation Group size (maximum number of ports) Also see Note 2 below	✓	8	8	24/48	24/48	24 (3.5.0) 64 (3.5.1)
Auto module max speed detection & notification	✓			✓	✓	
IP conflict detection & notification		✓	✓	✓	✓	✓
MAC-IP Binding	✓			✓	✓	✓
Static BFD					✓	✓
Hardware-based ECMP	N/A			✓	✓	✓
Private VLANs	✓		✓	✓	✓	✓
Loop-guard	✓	✓	✓	✓	✓	✓
LAG min-max-bundle		✓	✓	✓	✓	✓
SFLOW	✓	✓	✓	✓	✓	✓
Storm Control	✓	✓	✓	✓	✓	✓
ACL			✓	✓	✓	✓
Static L3/hardware-based routing	✓		✓	✓	✓	✓
Software Routing only	✓	✓				
CPLD Software Upgrade Support for OS					✓	
PoE-pre-standard detection (see Note 1 below)	✓	✓	✓	✓		
VLAN tag by ACL			✓	✓	✓	✓
ACL redirect to mirror destination as trunk/LAG			✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
MAC/IP/Protocol Based VLAN Assignment	✓	✓	✓	✓	✓	✓
802.1x port mode	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓		✓	✓	✓	✓
User based (802.1x) VLAN Assignment	✓	✓	✓	✓	✓	✓
Virtual Wire	✓	✓	✓	✓	✓	✓
HTTP REST APIs for Configuration and Monitoring	N/A	✓	✓	✓	✓	✓
Split Port				✓		✓
IGMP Snooping			✓	✓	✓	✓
Per-port max for learned MACs			✓	✓		
802.1p support, including Priority Queuing Trunk and WRED (release 3.5.1)			✓	✓	✓	✓
DHCP Snooping			✓	✓	✓	✓
LLDP-MED		✓	✓	✓	✓	✓
DHCP relay feature			✓	✓	✓	✓
Support for Switch SNMP OID		✓	✓	✓	✓	✓
802.1x Enhancements, including MAB (release 3.5.1)	✓	✓	✓	✓	✓	✓
Multi-stage Load Balancing (release 3.5.1)					✓	✓
MCLAG (Multichassis Link Aggregation)(release 3.6.0)		N/A	✓ (not on 124D/124D-POE)	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
Dynamic Layer 3 Protocols (OSPF, RIP, and VRRP) (release 3.6.0)	✓	N/A	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic ARP Inspection (release 3.6.0)		N/A	✓	✓	✓	✓
STP Root Guard(release 3.6.1)		✓	✓	✓	✓	✓
Firmware Image Rotation (Dual-firmware image support) (release 3.6.0)		✓ (not on 108D-POE, 224D-POE)	✓	✓	✓	✓
TDR (Time-Domain Reflectometer)/Cable Diagnostics Support (release 3.6.0)	✓	N/A	✓	✓	✓	✓
Per-VLAN MAC Learning Limit (release 3.6.0)		N/A	✓	✓		
Sticky MAC on Switch Interfaces (release 3.6.0)		N/A	✓	✓	✓	✓
PoE Modes Support: First Come, First Served or Priority Based (PoE models) (release 3.6.0)		✓	✓	✓	N/A	✓
ACL: Egress Mask Action support (release 3.6.0)		N/A	✓ (not on 248Ds, 448Ds)	✓	✓	✓
Monitor System Temperature (threshold configuration and SNMP trap support) (release 3.6.0)		✓	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)		✓	✓	✓	✓	✓
Selective Packet Sampling to CPU (useful diagnostic tool) (release 3.6.0)		N/A	✓	✓	✓	3.6.1
Add CLI to show the details of port statistics (release 3.6.0)		✓	✓	✓	✓	✓
Display Progress (%) During Firmware Upgrade (release 3.6.0)	✓	✓	✓	✓	✓	✓

Notes

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524_FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548_FPOE, and 1048D models.
3. To use the dynamic Layer 3 protocols, you must have an advanced features license.

Before You Begin

Before you start administrating your FortiSwitch unit, it is assumed that you have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch model and have administrative access to the FortiSwitch unit's web-based manager and CLI.

How this Guide is Organized

This guide is organized into the following chapters:

- Management Ports - configuring the management ports.
- Configuring Admin Tasks - configuring date and time, admin users, remote authentication servers.
- Configuring SNMP - allows you to monitor hardware on your network.
- Global System Settings - the initial configuration of your FortiSwitch unit.
- Physical Port Settings - configuring the physical ports.
- Layer 2 Interfaces - configuring Layer 2 interfaces.
- VLANs and VLAN Tagging - configuration and packet flow for VLAN-tagged and untagged packets.
- Spanning Tree Protocol - how to configure MSTP.
- Link Aggregation Groups - configuring Link Aggregation Groups.
- MCLAG - configuring MCLAG.
- Multi-Stage Load Balance - configuring multi-stage load balancing on a set of FortiGate units.
- LLDP-MED - how to configure LLDP-MED settings.
- MAC/IP/Protocol-based VLANs - configuring MAC/IP/Protocol-based VLANs.
- Mirroring - configuring port mirroring.
- Access Control Lists - configuring ACLs.
- Storm Control - configuring storm control.
- DHCP Snooping - configuring DHCP snooping.
- Dynamic ARP Inspection - configuring dynamic ARP inspection.
- IGMP Snooping - configuring IGMP snooping.
- Private VLANs - creation and management of private virtual local area networks (VLANs).
- QoS Settings - how to configure QoS.
- sFlow - configuring sFlow.
- Feature Licensing - about feature licenses.
- Layer 3 Interfaces - configuring routed ports, routed VLAN interfaces, switch virtual interfaces, and features related to these interfaces.
- DHCP Relay - configuring DHCP relay.
- OSPF Routing - configuring OSPF routing.
- RIP Routing - configuring RIP routing.
- VRRP Routing - configuring VRRP routing.
- Users and User Groups - configuring users and user groups.
- 802.1x Authentication - configuring 802.1x authentication (to RADIUS servers).
- TACACS - configuring TACACS authentication.

- Troubleshooting and Support
- Deployment Scenario

Management Ports

This chapter describes how to configure management ports on the FortiSwitch.

Models without Dedicated Management Port

For FortiSwitch models without a dedicated management port, configure the internal interface as the management port.

Note: For FortiSwitch models without a dedicated management port, the internal interface has a default VLAN ID of 1.

Using the web-based manager:

First start by editing the default **internal** interface's configuration.

1. Go to **System > Network > Interface** and edit the **internal** interface.
2. Assign an **IP/Netmask**.
3. Set **Administrative Access** to use the desired protocols to connect to the interface.
4. Select **OK**.

Next, create a new interface to be used for management.

1. Go to **System > Network > Interface** and select **Create New** to create a management VLAN**.**
2. Give the interface an appropriate name.
3. Set **Interface** to **internal**.
4. Set a **VLAN ID**.
5. Assign an **IP/Netmask**.
6. Set **Administrative Access** to use the desired protocols to connect to the interface.
7. Select **OK**.

Using the CLI:

```
config system interface
   edit internal
      set ip <address>
      set allowaccess <access_types>
      set type physical
   next
   edit <vlan name>
      set ip <address>
      set allowaccess <access_types>
      set interface internal
      set vlanid <VLAN id>
   end
end
```

Models with Dedicated Management Port

For FortiSwitch models with a dedicated management port, configure the IP address and allowed access types for the management port.

Note: For FortiSwitch models with a dedicated management port, the internal interface has a default VLAN id of 4094.

Using the web-based manager:

1. Go to **System > Network > Interface** and edit the **mgmt** interface.
2. Assign an **IP/Netmask**.
3. Set **Administrative Access** to use the desired protocols to connect to the interface.
4. Select **OK**.

Using the CLI:

```
config system interface
   edit mgmt
      set ip <address>
      set allowaccess <access_types>
      set type physical
   next
   edit internal
      set type physical
   end
end
```

Remote Access to Management Port

To provide remote access to the management port, configure a static route. Set the gateway address to the IP address of the router.

Using the web-based manager:

1. Go to **Router > Router > Static Route** and click **Create New**.
2. Set the device to **mgmt**.
3. Set the Gateway to the gateway router IP address.
4. Select **OK**.

Using the CLI:

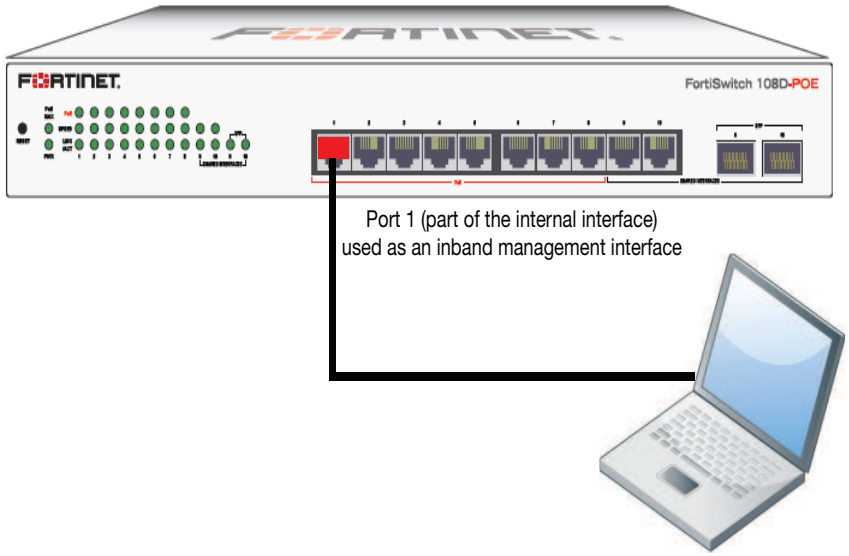
```
config router static
   edit 1
      set device mgmt
      set gateway <router IP address>
   end
end
```

Example Configurations

The following example configurations are for management ports, with the CLI syntax shown to create them.

In this example, the **internal** interface is used as an inbound management interface. Also, the FortiSwitch has a default VLAN across all physical ports and its internal port.

Using the internal interface of a FortiSwitch-108D-POE

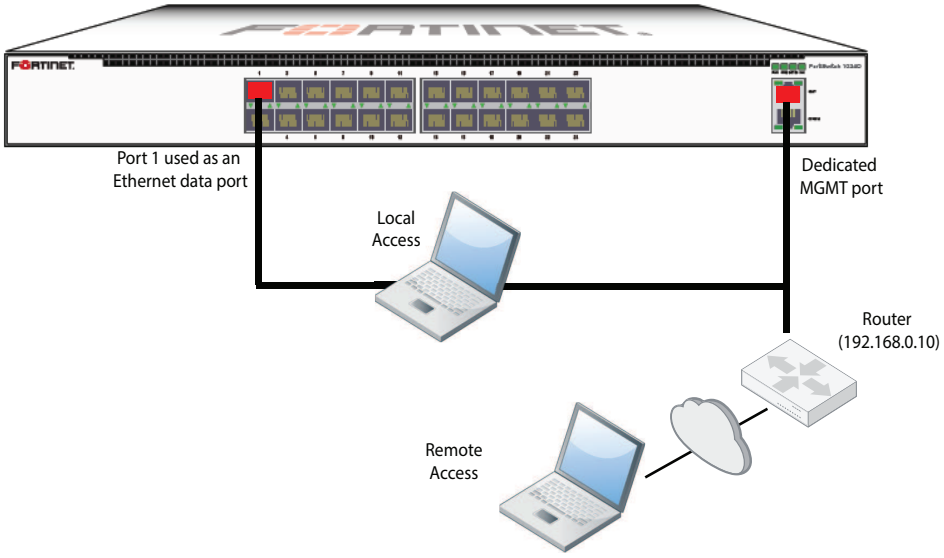


Syntax

```
config system interface
   edit internal
      set ip 192.168.1.99 255.255.255.0
      set allowaccess ping https http ssh
      set type physical
   end
end
```

In the example, an out-of-band management interface is used as the dedicated management port. You can configure the management port for local or remote access.

Out of band management on a FortiSwitch-1024D



Option 1: management port with static IP

```
config system interface
   edit mgmt
      set ip 10.105.142.19 255.255.255.0
      set allowaccess ping https http ssh snmp telnet
      set type physical
   next
   edit internal
      set type physical
   end
end
// optional configuration to allow remote access to the management port

config router static
   edit 1
      set device mgmt
      set gateway 192.168.0.10
   end
end
```

Option 2: management port with IP assigned by DHCP

```
config system interface
   edit mgmt
      set mode dhcp
```

```
      set defaultgw enable // allows remote access
      set allowaccess ping https http ssh snmp telnet
      set type physical
   next
   edit internal
      set type physical
   end
end
```

Configuring Admin Tasks

Setting Time and Date

For effective scheduling and logging, the system date and time must be accurate. You can either manually set the system date and time or configure the system to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

The Network Time Protocol enables you to keep the system time synchronized with other network systems. This will also ensure that logs and other time-sensitive settings are correct.

To set the date and time

1. Go to **System** > **Dashboard** and locate the **System Information** widget.
2. Beside **System Time,** select **Change**.
3. Select your **Time Zone**.
4. Either select **Set Time** and manually set the system date and time, or select **Synchronize with NTP Server**. If you select synchronization, you can either use the default FortiGuard servers or specify a different server. You can also set the **Sync Interval**.
5. Select **OK**.

If you use an NTP server, you can identify a specific port/IP address for this self-originating traffic. The configuration is performed in the CLI with the command `set source-ip`. For example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
   set ntpsyn enable
   set syncinterval 5
   set source-ip 192.168.4.5
end
```

Setting Thresholds for the System Temperature

You can set a warning and an alarm for when the system temperature reaches specified temperatures. When these thresholds are exceeded, a log message or SNMP trap is generated. The warning threshold must be lower than the alarm threshold.

Use the following commands to set warning and alarm thresholds:

```
config system snmp sysinfo
   set trap-temp-warning-threshold <number of degrees Celsius>
   set trap-temp-alarm--threshold <number of degrees Celsius>
end
```

Upgrading Firmware

You can upgrade the firmware from the dashboard or from the system configuration page.

To upgrade the firmware from the dashboard:

1. Go to **System** > **Dashboard** > **Status**
2. Next to the **Firmware Version** field, click the **Update** link.

To upgrade the firmware from the system configuration page:

1. Go to **System** > **Config** > **Firmware**
2. Click **Upgrade**.

Remote Authentication Servers

If you are using remote authentication for administrators or users, you need to configure the RADIUS or TACACS servers.

Radius Server

The information you need to configure the system to use a RADIUS server includes:

- the RADIUS server's domain name or IP address
- the RADIUS server's shared secret key

The default port for RADIUS traffic is 1812. Some RADIUS servers use port 1645. You can configure the FortiSwitch to use port 1645:

```
config system global
   set radius-port 1645
end
```

To configure RADIUS authentication with the web-based manager:

1. Go to **System** > **Authentication** > **RADIUS Servers** and select **Create New**.
2. Enter the following information and select **OK**.

Field	Description
Name	Enter a name to identify the RADIUS server on the FortiSwitch.
Type	Select **Query** or **Dynamic Start**.
Primary Server Name/IP	Enter the domain name (such as fgt.exmaple.com) or the IP address of the RADIUS server.

Field	Description
Primary Server Secret	Enter the server secret key, such as radiusSecret. This key can be a maximum of 16 characters long. This value must match the secret on the RADIUS primary server.
Secondary Server Name/IP	Optionally enter the domain name (such as fgt.exmaple.com) or the IP address of the secondary RADIUS server.
Secondary Server Secret	Optionally, enter the secondary server secret key, such as radiusSecret2. This key can be a maximum of 16 characters long. This value must match the secret on the RADIUS secondary server.
Authentication Scheme	If you know the RADIUS server uses a specific authentication protocol, select it from the list. Otherwise select **Use Default Authentication Scheme**. The Default option will usually work.
NAS IP/ Called Station ID	Enter the IP address to be used as an attribute in RADIUS access requests. **NAS-IP-Address** is RADIUS setting or IP address of the FortiSwitch interface used to talk to the RADIUS server, if not configured. **Called Station ID** is the same value as NAS-IP Address but in text format.
Include in every User Group	When enabled, this RADIUS server will automatically be included in all user groups. This option is useful if all users will be authenticating with the remote RADIUS server.

To configure the FortiSwitch for RADIUS authentication, see 802.1x Authentication.

TACACS Server

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices using one or more centralized servers. TACACS+ allows a client to accept a username and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

TACACS+ offers fully encrypted packet bodies and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP protocol.

To configure TACACS+ authentication using the web-based manager:

1. Go to **System** > **Authentication** > **TACACS Servers** and select **Create New**.
2. Enter the following information and select **OK**.

Field	Description
Name	Enter a name to identify the TACACS server on the FortiSwitch.
Server Name/IP	Enter the domain name (such as fgt.exmaple.com) or the IP address of the TACACS server.
Server Key	Enter the server key for the TACACS server.
Authentication Type	Select the authentication type to use for the TACACS+ server. **Auto** tries PAP, MSCHAP, and CHAP (in that order).

To configure the FortiSwitch for TACACS+ authentication, see TACACS.

Configuring System Administrators

Administrator profiles

Administer profiles define what the administrator user can do when logged into the FortiSwitch. When you set up an administrator user account, you also assign an administrator profile, which dictates what the administrator user will see. Depending on the nature of the administrator's work, access level, or seniority, you can allow them to view and configure as much, or as little, as required.

The super_admin administrator is the administrative account that the primary administrator should have to log into the FortiSwitch. The profile cannot be deleted or modified to ensure there is always a method to administer the FortiSwitch.This user profile has access to all components of the system, including the ability to add and remove other system administrators. For some administrative functions, such as backing up and restoring the configuration using SCP, super_admin access is required.

Creating Admin profiles

To configure administrator profiles go to **System** > **Admin Profiles**. You can only assign one profile to each administrator user.

On the **New Admin Profile** page, you define the components of FortiSwitch that will be available to view and/or edit. For example, if you configure a profile so that the administrator can only access System Configuration, this admin will not be able to change Network settings.

Using the web-based manager:

1. Go to **System > Admin > Admin Profile** and select **Create New**.
2. Give the profile an appropriate name.

3. Set **Access Control** as desired, choosing between **None**, **Read Only**, or **Read-Write.**
4. Select **OK**.

Using the CLI:

```
config system accprofile
   edit <name>
      set admingrp {none | read | read-write}
      set loggrp {none | read | read-write}
      set netgrp {none | read | read-write}
      set routegrp {none | read | read-write}
      set sysgrp {none | read | read-write}
   end
end
```

Adding Administrators

Only the default “admin” account can create a new administrator account. If required, you can add an additional account with read-write access control to add new administrator accounts.

If you log in with an administrator account that does not have the super_admin admin profile, the administrators list will show only the administrators for the current virtual domain.

When adding administrators, you are setting up the administrator’s user account. An administrator account comprises an administrator’s basic settings as well as their access profile. The access profile is a definition of what the administrator is capable of viewing and editing.

Follow these steps to add an administrator.

Using the web-based manager:

1. Go to **System** > **Administrators**.
2. Select **Create New**.
3. Enter the administrator name.
4. Select the type of account. If you select **Remote**, the system can reference a RADIUS or TACAS+ server.
5. When selecting Remote or PKI accounts, select the User Group the account will access.
6. Enter the password for the user. Passwords can be up to 256 characters in length.
7. Select **OK**.

Using the CLI:

```
config system admin
   edit <admin_name>
      set password <password>
      set accprofile <profile_name>
   end
```

Monitoring Administrators

You can view the administrators logged in using the **System Information** widget on the **Dashboard**. On the widget is the **Current Administrator** row that shows the administrator logged in and the total logged in.

Selecting **Details** displays the information for each administrator: where they are logging in from and how (CLI, web-based manager) and when they logged in.

You are also able to monitor the activities the administrators perform using Event Logging. Event logs include a number of options to track configuration changes.

To set logging using the web-based manager:

1. Go to **Log** > **Log Config** > **Log Settings**.
2. Under **Event Logging**, ensure that **System activity event** is selected.
3. Select **Apply**.

To set logging using the CLI:

```
config log eventfilter
   set event enable
   set system enable
end
```

To view the logs, go to **Log** > **Event Log** > **System**.

Default administrator password

By default, your system has an administrator account set up with the user name `admin` and no password. To prevent unauthorized access, it is highly recommended that you add a password to this account.

To change the default password:

1. Go to **System** > **Administrators**.
2. Edit the **admin** account.
3. Select **Change Password**.
4. Leave **Old Password** blank, enter the **New Password** and re-enter the password for confirmation.
5. Select **OK**.

Administrator password retries and lockout time

By default, the system includes a set number of three password retries, allowing the administrator a maximum of three attempts to log into their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts can be set to an alternate value, as well as the default wait time before the administrator can try to enter a password again. You can also change this value to make it moredifficult to hack. Both settings are must be configured with the CLI

To configure the lockout options:

```
config system global
   set admin-lockout-threshold <failed_attempts>
   set admin-lockout-duration <seconds>
end
```

For example, to set the lockout threshold to one attempt and the duration before the administrator can try again to log in to five minutes, enter these commands:

```
config system global
   set admin-lockout-threshold 1
   set admin-lockout-duration 300
end
```

Idle timeout and Other Admin Settings

By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management PC is left unattended.

To change the idle timeout

1. Go to **System** > **Admin** > **Settings**
2. Enter the time in minutes in the **Idle Timeout** field.
3. Update other settings as required:
   - TCP/UDP port values for HTTP, HTTPS, Telnet, SSH
   - Display language
4. Select **Apply**.

Configuring Security Feature Settings

You can enable the following security checks for incoming TCP/UDP packets. The packet is dropped if the system detects the specified condition.

Syntax (for models FS108D-POE, FS112D-POE, FS224D-POE)

```
config switch security-feature
   set tcp-syn-data {enable | disable}
   set tcp-udp-port-zero {enable | disable}
   set tcp_flag_zero {enable | disable}
   set tcp_flag_FUP {enable | disable}
   set tcp_flag_SF {enable | disable}
   set tcp_flag_SR {enable | disable}
   set tcp_frag_ipv4_icmp {enable | disable}
   set tcp_arp_mac_mismatch {enable | disable}
```

Variable	Description	Default
tcp-syn-data	TCP SYN packet contains additional data (possible DoS attack).	disable
tcp-udp-port-zero	TCP or UDP packet has source or destination port set to zero.	disable
tcp_flag_zero	TCP packet with all flags set to zero.	disable

Variable	Description	Default
tcp_flag_FUP	TCP packet with FIN, URG and PSH flag set.	disable
tcp_flag_SF	TCP packet with SYN and FIN flag set.	disable
tcp_flag_SR	TCP packet with SYN and RST flag set.	disable
tcp_frag_ipv4_icmp	Fragmented ICMPv4 packet.	disable
tcp_arp_mac_mismatch	ARP packet with MAC source address mismatch between the Layer 2 header and the ARP packet payload.	disable

Syntax (for all other FortiSwitch models)

```
config switch security-feature
   set sip-eq-dip {enable | disable}
   set tcp-flag {enable | disable}
   set tcp-port-eq {enable | disable}
   set tcp-flag-FUP {enable | disable}
   set tcp-flag-SF {enable | disable}
   set v4-first-frag {enable | disable}
   set udp-port-eq {enable | disable}
   set tcp-hdr-partial {enable | disable}
   set macsa-eq-macda {enable | disable}
```

Variable	Description	Default
sip-eq-dip	TCP packet with source IP equal to destination IP.	disable
tcp_flag	DoS attack checking for TCP flags.	disable
tcp-port-eq	TCP packet with source and destination TCP port equal.	disable
tcp-flag-FUP	TCP packet with FIN, URG, and PSH flags set, and sequence number is zero.	disable
tcp-flag-SF	TCP packet with SYN and FIN flag set.	disable
v4-first-frag	DoS attack checking for IPv4 first fragment.	disable
udp-port-eq	IP packet with source and destination UDP port equal.	disable
tcp-hdr-partial	TCP packet with partial header.	disable
macsa-eq-macda	Packet with source MAC equal to destination MAC.	disable

Configuring SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network.

The FortiSwitch SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiSwitch system information through queries and can receive trap messages from the FortiSwitch.

To monitor FortiSwitch system information and receive FortiSwitch traps, you must first compile the Fortinet and FortiSwitch Management Information Base (MIB) files. A MIB is a text file that describes a list of SNMP data objects that are used by the SNMP manager. These MIBs provide information that the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiSwitch SNMP agent.

FortiSwitch core MIB files are available for download by going to **System** > **Config** > **SNMP** and selecting the MIB download link.

SNMP Access

Ensure that the management vlan has SNMP added to the access-profiles.

Using the web interface:

1. Go to **System** > **Network** > **Interface**.
2. Edit the management interface.
3. Set **SNMP** in the access profiles.
4. Select **Apply**.

Using the CLI:

```
config system interface
   edit <name>
      set allowaccess <access_types>
   end
end
```

Note: re-enter the existing allowed access types, and add **snmp** to the list.

SNMP Agent

Create the SNMP agent.

Using the web interface:

1. Go to **System** > **Config** >**SNMP**.
2. Click **Enable** for the SNMP Agent.

3. Enter a descriptive name for the agent.
4. Enter the location of the FortiGate unit.
5. Enter a contact or administrator for the SNMP Agent or FortiSwitch unit.
6. Select **Apply**.

Using the CLI:

```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiSwitch>
   set location <FortiSwitch_location>
end
```

SNMP Community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a FortiGate SNMP and a FortiSwitch SNMP community.

Add SNMP communities to your FortiSwitch so that SNMP managers can connect to view system information and receive SNMP traps.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiSwitch for a different set of events. You can also add the IP addresses of up to 8 SNMP managers for each community.

Adding an SNMP v1/v2c community

Using the web interface:

1. Go to **System** > **Config** > **SNMP**.
2. In the SNMP v1/v2c area, select **Create New**.
3. Enter a community name.
4. Enter the IP address and identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiSwitch.
5. Select the interface if the SNMP manager is not on the same subnet as the FortiSwitch.
6. Enter the port number that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiSwitch. Select the **Enable** check box to activate queries for each SNMP version.
7. Enter the local and remote port numbers that the FortiSwitch uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community.
8. Select the **Enable** check box to activate traps for each SNMP version.
9. Select **OK**.

Using the CLI:

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-lport <port_number>
      set trap-v1-rport <port_number>
      set trap-v1-status {enable | disable}
      set trap-v2c-lport <port_number>
      set trap-v2c-rport <port_number>
      set trap-v2c-status {enable | disable}
```

Adding an SNMP v3 community

Using the web interface:

1. Go to **System** > **Config** > **SNMP**.
2. In the SNMP v3 area, select **Create New**.
3. Enter a User Name.
4. Select a Security Level and associated authorization algorithms.
5. Enter the IP address of the Notification Host SNMP managers that can use the settings in this SNMP community to monitor the FortiSwitch.
6. Enter the Port number that the SNMP managers in this community use to receive configuration information from the FortiGate unit. Select the **Enable Query** check box to activate queries for each SNMP version.
7. Select the events to report.
8. Select **OK**.

Using the CLI:

```
config system snmp user
   edit <index_number>
      set events <event_selections>
      set queries enable
      set query-port <port_number>
      set security-level [auth-priv | auth-no-priv | no-auth-no-priv}
   end
```

Global System Settings

Configuration File Settings

You can set preferences for the configuration files:

1. Go to **System** > **Config** > **Settings**
2. Select a value for Configuration Save:
   - **Auto** - system automatically saves the configuration after each change.
   - **Manual** - you must manually save configuration changes, from **System** > **Config** > **Revisions**.
   - **Revertive** - you must manually save configuration changes. System reverts to the saved configuration after a timeout. You can set the timeout using the CLI:
     ```
     config system global
     set cfg-revert-timeout <integer>
     ```
3. If you select **Revision Backup on Logout**, the FortiSwitch will create a configuration file each time a user logs out.
4. If you select **Revision Backup on Upgrade**, the FortiSwitch will create a configuration file before starting a system upgrade.
5. If you select **Strong Crypto**, the configuration is stored encrypted with strong cryptography.
6. Click **Apply**.

Configuration File Revisions

Using the web-based manager:

1. Go to **System** > **Config** > **Revisions**
   The system displays a new page with an entry for each configuration file revision.
2. When you select a revision, the following commands are available:
   - **Delete** - deletes the revision file.
   - **Details** - displays the contents of the revision file.
   - **Change** Comments - to edit the comments field for this revision file.
   - **Revert** - reverts the system configuration to use this revision file.
   - **Upload** - uploads the revision file to your local machine.
3. If you select two revision files, click **Diff** to display the differences between the two files.

Using the CLI:

Use the following command to display the list of configuration file revisions:

```
execute revision list config
```

The FortiSwitch assigns a numerical ID to each configuration file. To display a particular configuration file contents, use the following command and specify the ID of the configuration file:

```
execute revision show config id <ID number>
```

The following example displays the list of configuration file revisions:

```
# execute revision list config

ID TIME ADMIN FIRMWARE VERSION COMMENT
1 2015-08-31 11:11:00 admin V3.0.0-build117-REL0 Automatic backup (session
expired)
2 1969-12-31 16:06:29 admin V3.0.0-build150-REL0 baseline
3 2015-08-31 15:19:31 admin V3.0.0-build150-REL0 baseline
4 2015-08-31 15:28:00 admin V3.0.0-build150-REL0 with admin timeout
```

The following example displays the configuration file contents for revision ID 62:

```
# execute revision show config id 62

#config-version=FS1D24-3.04-FW-build171-160201:opmode=0:vdom=0:user=admin
#conf_file_ver=1784779075679102577
#buildno=0171
#global_vdom=1
config system global
   set admin-concurrent enable
       ...
   (output truncated)
```

IP Conflict Detection

IP conflicts can occur when two systems on the same network are using the same IP address. FortiSwitch monitors the network for conflicts and raises a system log message and an SNMP trap when it detects a conflict.

Description

The IP Conflict Detection feature provides two methods to detect a conflict. The first method relies on a remote device to send a broadcast ARP (Address Resolution Protocol) packet claiming ownership of a particular IP address. If the IP address in the source field of that ARP packet matches any of the system interfaces associated with the receiving FortiSwitch system, the system logs a message and raises an SNMP trap.

For the second method, the FortiSwitch actively broadcasts gratuitous ARP packets when any of the following events occurs:

- System boot-up
- Interface status changes from down to up
- IP address change

If a system is using the same IP address, the FortiSwitch will receive a reply to the gratuitous ARP. If it receives a reply, the system logs a message.

Configuring IP Conflict Detection

IP conflict detection is enabled on a global basis. The default setting is enabled.

Using the web-based manager:

1. Go to **Network > Settings**.
2. Set **IP Conflict Detection**
3. Select **OK.**

Using the CLI:

```
config system global
   set detect-ip-conflict <enable|disable>
```

Viewing IP Conflict Detection

If the system detects an IP conflict, the system generates the following log message:

```
IP Conflict: conflict detected on system interface mgmt for IP address 10.10.10.1
```

Port Flap Guard

A flapping port can create instability in protocols such as STP. If a port is flapping, STP must continually recalculate the role for each port.

The port flap guard feature will detect a flapping port, and the system will shut down the port if necessary. You can manually reset the port and restore it to the enabled state.

Configuring Port Flap Guard

Port flap guard is configured and enabled on a global basis. The default setting is disabled. Flap rate ranges from 5 to 300.

Using the web-based manager:

1. Go to **Switch > Flap Guard > Settings**.
2. Enable **Flap Guard**.
3. Enter a value for **Flap duration** and **Flap rate**.
4. Click **Apply** to save the changes.

Using the CLI:

```
config switch flapguard settings
   set status [ disable | enable ]
   set flap-rate <integer>
   set flap-duration <integer>
```

Use the following command to reset a port and restore it to service:

```
execute flapguard reset <port>
```

Viewing Port Flap Guard Configuration

Display the status of the port flap guard configuration using the following command:

```
show switch flapguard settings
```

Display the port flap guard information for each port using the following command:

```
diagnose flapguard instance status
```

Link Monitor

You can monitor the link to a server. The FortiSwitch sends periodic ping messages to test that the server is available.

Configuring Link Monitor

Using the web-based manager:

1. Go to **Router > Link Monitor > Probes**.
2. Click **Create New** to create a new probe.
3. Enter an IP address for the **Gateway IP**.
4. Configure the other fields as required (see table below for field descriptions).
5. Click **Advance Settings** to view additional fields that you can configure.
6. Click **OK** to save the changes.

Using the CLI:

```
config system link-monitor
   edit "1"
      set srcintf <string>
      set protocol (arp | ping)
      set gateway-ip <IP address>
      set source-ip <IP address>
      set interval <integer>
      set timeout <integer>
      set failtime <integer>
      set recoverytime <integer>
      set update-cascade-interface (enable | disable)
      set update-static-route (enable | disable)
      set status (enable | disable)
   next
end
```

Variable	Description
srcintf	Interface where the monitor traffic is sent.
protocol	Protocols used to detect the server. Select ARP or ping.
gateway-ip	Gateway IP used to PING the server.
source-ip	Source IP used in packet to the server.
interval	Detection interval in seconds. The range is 1-3600.
timeout	Detect request timeout in seconds. The range is 1-255.
failtime	Number of retry attempts before bringing the server down. The range is 1-10.
recoverytime	Number of retry attempts before bringing the server up. The range is 1-10.
update-cascade-interface	Enable/disable update cascade interface.
update-static-route	Enable/disable update static route.
status	Enable/disable link monitor administrative status.

Physical Port Settings

This following sections describe the configuration settings that are associated with FortiSwitch physical ports:

- General port settings
- Flow Control
- Auto-Module Speed Detection
- Speed
- Power over Ethernet
- DMI Module Status
- Split Port

Configuring General Port Settings

Using the web-based manager:

1. Go to **Switch > Physical > Interface** and select the port to update.
2. Enter values for Name and Description.
3. Select the Admin port status.
4. Select **OK.**

Using the CLI:

```
config switch physical-port
   edit <port>
      set description <string>
      set max-frame-size
      set status (up | down)
```

General port settings include:

- **description** - Text description for the port
- **max-frame-size** - Maximum frame size in bytes (between 68 and 9216)
- **status** - Administrative status of the port

Viewing Port Statistics

Use the following command to get statistics for a specific port:

```
diag switch physical-ports port-stats <port_number>
```

For example:

```
diag switch physical-ports port-stats port1
```

Configuring Flow Control

Flow control represents the ability to configure a port to send or receive a “pause frame” (that is, a special packet that signals a source to stop sending flows for a specific time interval because the buffer is full):

```
config switch physical-port
   edit <port>
      set flow-control (both | rx | tx | disable)
```

Parameters enable flow control to do the following:

- **rx** - receive pause control frames
- **tx** - transmit pause control frames
- **both** - transmit and receive pause control frames

Auto-Module Speed Detection

When you enable auto-module speed detection, the system reads information from the module and sets the port speed to the maximum speed that is advertised by the module. If the system encounters a problem when reading from the module, it sets the default speed (default value is platform specific).

When auto-module sets the speed, the system creates a log entry noting this speed.

NOTE: Auto-speed detection is supported on 1/10G ports, but not on higher speed ports (such as 40G).

Setting Port Speed (Autonegotiation)

By default, all of the FortiSwitch user ports are set to autonegotiate the port speed. You can also manually set the port speed:

Using the web-based manager:

1. Go to **Switch > Port > Physical** and select the port.
2. Click **Edit**.
3. Select the desired port speed.
4. Click **OK**.

Using the CLI:

```
config switch physical-port
   edit <port>
      set speed (auto | 10full | 10half | 100full | 100half | 1000auto)
   end
end
```

Viewing Auto-Module Configuration

Display the status of auto-module using following command:

```
config switch physical-port
   edit port47
      show
   config switch physical-port
      edit "port47"
         set max-frame-size 16360
         set speed 10000full
      next
   end
get
   name : port47
   description : (null)
   flow-control : both
   link-status : down
   lldp-transmit : disable
   max-frame-size : 16360
   port-index : 47
   speed : 10000full
   status : up
```

Link-Layer Discovery Protocol

The Fortinet data center switches support LLDP (transmission and reception). The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that enables devices on a Layer 2 segment to discover information about each other.

For details, refer to LLDP-MED.

Configuring Power over Ethernet

Power over Ethernet (PoE) describes any system that passes electric power along with data on twisted pair Ethernet cabling. Doing this allows a single cable to provide both data connection and electric power to devices (for example, wireless access points, IP cameras, and VoIP phones).

PoE is only available on models with the POE suffix in the model number (for example, FS-108D-POE).

Enabling PoE on a Port

```
config switch physical-port
   edit <port>
      set poe-status enable
      set poe-pre-standard-detection {enable | disable}
```

```
      set poe-reset reset
   end
end
```

Determining the PoE Power Capacity

To determine the PoE power capacity, use the following command:

```
get switch poe inline
```

Reset the PoE Power on a Port

To reset the PoE power on a port, use the following command:

```
execute poe-reset <port>
```

Selecting How Power Is Allocated

When power to PoE ports is allocated by priority, lower numbered ports have higher priority so that port 1 has the highest priority. When more power is needed than is available, higher numbered ports are disabled first.

When power to PoE ports is allocated by first-come, first-served (FCFS), connected PoE devices receive power, but new devices do not receive power if there is not enough power.

If both priority power allocation and FCFS power allocation are selected, the physical port setting takes precedence over the global setting.

To select priority power allocation on a global basis, use the following command:

```
config switch global
   set poe-port-mode priority
end
```

To select FCFS power allocation on a global basis, use the following command:

```
config switch global
   set poe-port-mode first-come-first-served
end
```

To set the priority (from low to critical) for priority power allocation for a specific port, use the following command:

```
config switch physical-port
   edit <port>
      set poe-port-priority <priority>
```

Configure PoE with Dynamic Guard Band (DGB)

The dynamic guard band is set automatically to the expected power of a port before turning on the port. So, when a PoE device is plugged in, the dynamic guard band is set to the maximum power of the device type based on the AF or AT mode. The AF mode DGB is 15.4 W, and the AT mode DGB is 36 W. When the FS-224D-POE is fully loaded, the dynamic guard band prevents a new PoE device from turning on.

To avoid this issue, change the port mode using the following commands:

```
config switch physical-port
   edit <port>
```

```
    set port-mode IEEE802_3AF
end
```

Display PoE information for a Port

To display PoE information for a port, use the following command:

```
diagnose switch poe status <port>
```

The following example displays the information for port 6:

```
diagnose switch poe status port6
Port(6) Power:4.20W, Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AT PD
Power Class: 4
Defined Max Power: 30.0W, Priority:3
Voltage: 54.00V
Current: 71mA
```

Diagnostic Monitoring Interface Module Status

With Diagnostic Monitoring Interface (DMI), you can view the following information

- Module details (detail)
- Eeprom contents (eeprom)
- Module limits (limit)
- Module status (status)
- Summary information of all a port's modules (summary)

Diagnostic Monitoring Interface (DMI) is supported on all models except FortiSwitch 124D.

Using the web-based manager:

Go to **Switch > Monitor > Modules**.

Using the CLI:

Use the following commands to enable or disable DMI status for the port. If you set the status to **global**, the port setting will match the global setting:

```
config switch physical-port
   edit <interface>
      set dmi-status {disable | enable | global}
```

Use the **get switch modules detail/status** command to display DMI information:

```
S524DF4K15000002 # get switch modules detail
_____________________________________________________
Port(port25)
identifier      SFP/SFP+
connector       LC
transceiver     1000-Base-SX
encoding        8B/10B
Length Decode Common
 length_smf_1km  N/A
 length_cable    N/A
SFP Specific
 length_smf_100m N/A
 length_50um_om2 550 meter
 length_62um_om1 270 meter
 length_50um_om3 N/A
vendor          AVAGO
vendor_oid      0x00176A
vendor_pn       AFBR-5710PZ
vendor_rev
vendor_sn       AM15372BH3C
manuf_date      09/09/2015
```

Below is an example output for the command switch modules status:

```
FS1D483Z14000142 # get switch modules status
_____________________________________________________
Port(port1)
Empty
.
.
.

_____________________________________________________
Port(port15)
alarm_flags     0x0040
warning_flags   0x0040
temperature     33.847656 C
voltage         3.316700 volts
laser_bias      0.554800 mAmps
tx_power        -2.270918 dBm
rx_power        -40.000000 dBm
options         0x000F ( TX_DISABLE TX_FAULT RX_LOSS TX_POWER_LEVEL1 )
options_status  0x000C ( RX_LOSS TX_POWER_LEVEL1 )

_____________________________________________________
Port(port16)
alarm_flags     0x0040
warning_flags   0x0040
temperature     33.957031 C
voltage         3.314100 volts
laser_bias      0.561000 mAmps
tx_power        -2.241712 dBm
rx_power        -40.000000 dBm
options         0x000F ( TX_DISABLE TX_FAULT RX_LOSS TX_POWER_LEVEL1 )
options_status  0x000C ( RX_LOSS TX_POWER_LEVEL1 )
```

Configuring Split Port

On FortiSwitch models that provide 40G QSFP (Quad Small Form-factor Pluggable) interfaces, you can install a breakout cable to convert one 40G interface into four 10G interfaces.

Notes

1. Split Port is supported on the following FortiSwitch models:
   - 3032D (port5 to port28 are splittable)
   - 524D, 524D-FPOE (port29 and port30 are splittable)
   - 548D, 548D-FPOE (port53 and port54 are splittable)
2. Currently, the maximum number of ports supported in software is 64. Therefore, we cannot split more then 10 QSFP ports. This limitation applies to all of the models, but only the 3032D has enough ports to encounter this limit.
3. Split port is not supported in FortiLink mode (that is, FortiSwitch managed by FortiGate).

Configuration Commands

Use the following commands to configure split port:

```
config switch phy-mode
   set port-configuration <default | disable-port54 | disable-port41-48>
   set <port-name>-phy-mode <1x40G | 4x10G>
   ...
   (one entry for each port that supports split port)
end
```

NOTE: The **port-configuration** command applies solely to the 548D and 548D-FPOE models.

The following settings are available:

- **disable-port54** - only port53 is splittable; port54 is unavailable.
- **disable-port41-48** - port41 to port48 are unavailable, but you can configure port53 and port54 in split-mode.

In the following example, a FortiSwitch 3032D is configured with ports 10, 14, and 28 set to 4x10G:

```
config switch phy-mode
   set port5-phy-mode 1x40G
   set port6-phy-mode 1x40G
   set port7-phy-mode 1x40G
   set port8-phy-mode 1x40G
   set port9-phy-mode 1x40G
   set port10-phy-mode 4x10G
   set port11-phy-mode 1x40G
   set port12-phy-mode 1x40G
   set port13-phy-mode 1x40G
   set port14-phy-mode 4x10G
   set port15-phy-mode 1x40G
   set port16-phy-mode 1x40G
   set port17-phy-mode 1x40G
   set port18-phy-mode 1x40G
   set port19-phy-mode 1x40G
   set port20-phy-mode 1x40G
```

```
    set port21-phy-mode 1x40G
    set port22-phy-mode 1x40G
    set port23-phy-mode 1x40G
    set port24-phy-mode 1x40G
    set port25-phy-mode 1x40G
    set port26-phy-mode 1x40G
    set port27-phy-mode 1x40G
    set port28-phy-mode 4x10G
end
```

The system applies the configuration only after you enter the **end** command, displaying the following message:

```
This change will cause a ports to be added and removed, this will cause loss of
    configuration on removed ports. The system will have to reboot to apply this change.
Do you want to continue? (y/n)y
```

To configure one of the split ports, use the notation ".x" to specify the split port:

```
config switch physical-port
   edit "port1"
      set lldp-profile "default-auto-isl"
      set speed 40000full
   next
   edit "port2"
      set lldp-profile "default-auto-isl"
      set speed 40000full
   next
   edit "port3"
      set lldp-profile "default-auto-isl"
      set speed 40000full
   next
   edit "port4"
      set lldp-profile "default-auto-isl"
      set speed 40000full
   next
   edit "port5.1"
      set speed 10000full
   next
   edit "port5.2"
      set speed 10000full
   next
   edit "port5.3"
      set speed 10000full
   next
   edit "port5.4"
      set speed 10000full
   next
```

Layer 2 Interfaces

Configuring Switched Interfaces

Default configuration will suffice for regular switch ports. By default, VLAN is set to 1, STP is enabled, and all other optional capabilities are disabled.

You can configure optional capabilities such as Spanning Tree Protocol, sFlow 802.1x Authentication, and Private VLANs. These capabilities are covered in subsequent sections of this document.

Using the web-based manager:

1. Go to **Switch > Interface > Interface.**
2. Select the port to update and click **Edit**.
3. Select one or more ports to update and click **Edit**.
4. If you selected more than one port, the port names are displayed in the name field, separated by commas.
5. Enter new values as required for Native VLAN, Allowed VLANs and Untagged VLANs.
6. Click **OK** to save the changes.

Using the CLI:

```
config switch interface
   edit <port>
      set native-vlan <vlan>
      set allowed-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
      set untagged-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
      set stp-state {enabled | disabled}
      set edge-port {enabled | disabled}
      set security-mode {none| dot1x}
```

Dynamic MAC Address Learning

You can enable or disable dynamic MAC address learning on a port. The existing dynamic MAC entries are flushed when you change this setting. If you disable MAC address learning, you can set the behavior for an incoming packet with an unknown MAC address (to drop or forward the packet).

You can limit the number of learned MAC addresses on an interface. The limit ranges from 1 to 128. If the mac-limit is set to zero (the default), no limit exists. **NOTE:** Static MAC addresses are not counted in the limit. The limit refers only to learned MAC addresses.

Use the following CLI commands to configure Dynamic MAC Address Learning:

```
config switch physical-port
   edit <port>
      set l2-learning (enable | disable)
      set l2-unknown (drop | forward)
   end
config switch interface
   edit <port>
```

```
      set learning-limit <0 - 128>
   end
```

Note: If you enable 802.1x MAC-based authorization on a port, you cannot change the **l2_learning** setting.

By default, each learned MAC address is aged out after 300 seconds. The value ranges from 10 to 1000,000 seconds. Set the value to zero to disable MAC address aging.

Use the following command to change this value:

```
config switch global
   set mac-aging-interval 200
end
```

Setting Static MAC Addresses

You can configure one or more static MAC addresses on an interface.

Using the web-based manager:

1. Go to **Switch > Static L2 > Entries**.
2. Click **Create** to create a new item.
3. Select an interface, and enter a value for **MAC Address** and **VLAN ID**.
4. Click **Apply** to save the changes.

Using the CLI:

```
config switch static-mac
   edit "1"
      set interface <port>
      set mac <MAC address>
      set vlan-id <VLAN ID>
```

Setting Persistent MAC Addresses

You can make dynamically learned MAC addresses persistent when the status of a FortiSwitch port changes (goes down or up). By default, MAC addresses are not persistent.

Use the following command to configure the persistence of MAC addresses on an interface:

```
config switch interface
   edit <port>
      set sticky-mac <enable | disable>
   next
end
```

You can also save persistent MAC addresses so that they are automatically loaded when a FortiSwitch is rebooted. By default, persistent entries are lost when a FortiSwitch is rebooted. Use the following command to save persistent MAC addresses for all interfaces:

```
execute sticky-mac save
```

Use the following command to clear the current list of persistent MAC addresses:

```
execute sticky-mac clear
```

Viewing Interface Configuration

Display port configuration using the following command:

```
show switch interface <port>
```

Display port settings using following command:

```
config switch interface
   edit <port>
      get
```

Fortinet Loop Guard

A loop in a Layer 2 network results in broadcast storms that have far-reaching and unwanted effects. Fortinet Loop Guard helps to prevent loops. When Loop Guard is enabled on a switch port, the port monitors its subtending network for any downstream loops.

The loop guard feature is designed to work in concert with STP rather than as a replacement for STP. Each port that has loop guard enabled will periodically broadcast Loop Guard Data Packets (LGDP) packets to its network. If a broadcast packet is subsequently received by the sending port, a loop exists downstream.

NOTE: If a port detects a loop, the system takes the port out of service to protect the overall network. The port returns to service after a configured timeout duration. If the timeout value is zero, you must manually reset the port.

By default, Loop Guard is disabled on all ports, and the timeout is set to zero.

Configuring Loop Guard

Using the web-based manager:

1. Go to **Switch > Interface > Interface** or **Switch > Interface > Trunk**.
2. Select the port to update and click **Edit**.
3. Select one or more ports to update and click **Edit**.
4. If you selected more than one port, the port names are displayed in the name field, separated by commas.
5. Click **Enable Loop Guard**.
6. Click **OK**.

Using the CLI:

```
config switch interface
   edit port <number>
      set loop-guard <enabled|disabled>
      set loop-guard-timeout <integer>
```

When Loop Guard takes a port out of service, the system creates the following log messages:

```
Loop Guard: loop detected on <port_name>. Shutting down <port_name>
```

Use the following command to reset a port that detected a loop:

```
execute loop-guard reset <port>
```

Viewing Loop Guard Configuration

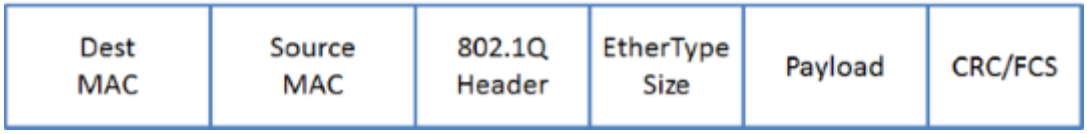
Use the following command to display the Loop Guard status for all ports:

```
diagnose loop-guard instance status
```

VLANs and VLAN Tagging

FortiSwitch ports will process tagged and untagged Ethernet frames. Untagged frames do not carry any VLAN information.

Tagged frames include an additional header (the 802.1Q header) after the Source MAC address. This header includes a VLAN ID. This allows the VLAN value to be transmitted between switches.



The FortiSwitch provides port parameters to configure and manage VLAN tagging.

Native VLAN

You can configure a native VLAN for each port. The native VLAN is like a default VLAN for untagged incoming packets. Outgoing packets for the native VLAN are sent as untagged frames.

The native VLAN is assigned to any untagged packet arriving at an ingress port.

At an egress port, if the packet tag matches the native VLAN, the packet is sent out without the VLAN header.

Allowed VLAN List

The Allowed VLAN list for each port specifies the VLAN tag values for which the port can transmit or receive packets.

For a tagged packet arriving at an ingress port, the tag value must match a VLAN on the Allowed VLAN list or the native VLAN.

At an egress port, the packet tag must match the native VLAN or a VLAN on the Allowed VLAN list.

Untagged VLAN List

The Untagged VLAN list on a port specifies the VLAN tag values for which the port will transmit packets without the VLAN tag. Any VLAN in the Untagged VLAN list must also be a member of the Allowed VLAN list.

The Untagged VLAN list applies only to egress traffic on a port.

Packet Processing

Ingress processing ensures that the port accepts only packets with allowed VLAN values (untagged packets are assigned the native VLAN, which is implicitly allowed). At this point, all packets are now tagged with a valid VLAN.

The packet is sent to each egress port that can send the packet (because the packet tag value matches the native VLAN or an Allowed VLAN on the port).

Ingress Port

Untagged packet

- packet is tagged with the native VLAN and allowed to proceed
- the Allowed VLAN list is ignored

Tagged packet

- tag VLAN value must match an Allowed VLAN or the native VLAN
- packet retains the VLAN tag and is allowed to proceed

To control what types of frames are accepted by the port, use the following commands:

```
config switch interface
   edit <interface>
      set discard-mode <all-tagged | all-untagged | none>
   end
```

Variable	Description
all-tagged	Tagged frames are discarded, and untagged frames can enter the switch.
all-untagged	Untagged frames are discarded, and tagged frames can enter the switch.
none	By default, all frames can enter the switch, and no frames are discarded.

Egress Port

All packets that arrive at an egress port are tagged packets.

If the packet tag value is on the Allowed VLAN list, the packet is sent out with the existing tag.

If the packet tag value is the native VLAN or on the Untagged VLAN list, the tag is stripped, and then the packet is sent out.

Otherwise, the packet is dropped.

Configuring VLANs

Use the following steps to create a new VLAN interface:

Using the web-based manager:

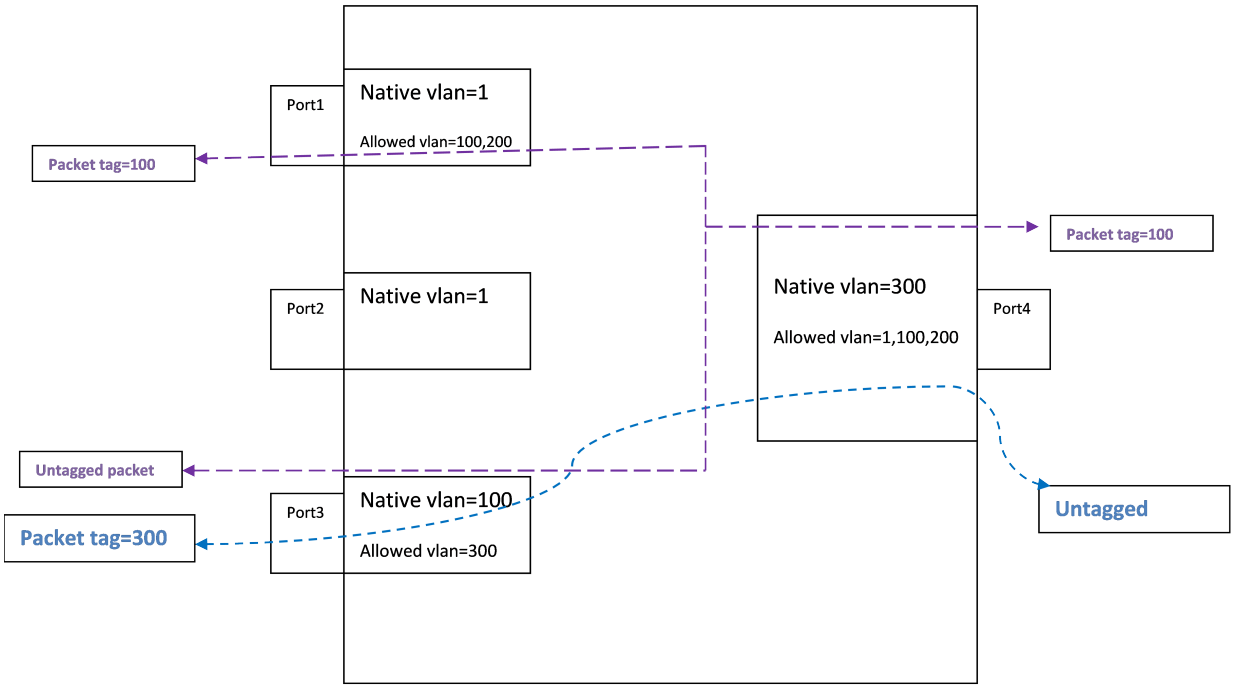
1. Go to **System > Network > Interface** and select **Create New** to create a VLAN.
2. Give the VLAN an appropriate name.
3. Set **Interface** to **internal**.
4. Set a **VLAN ID**.
5. Assign an **IP/Netmask**.
6. Set **Administrative Access** to use the desired protocols to connect to the interface.
7. Select **OK**.

Using the CLI:

```
config system interface
   edit <vlan name>
      set ip <address>
      set allowaccess <access_types>
      set switch-members <port>
      set vlanid <VLAN id>
   end
end
```

Example 1

Example flows for tagged and untagged packets.



Purple flow:

An untagged packet arriving at Port3 is assigned VLAN 100 (the native VLAN) and flows to all egress ports that will send VLAN 100 (Port1 and Port4).

A tagged packet (VLAN 100) arriving at Port4 is allowed (VLAN 100 is allowed). The packet is sent out from Port1 and Port3. On Port3, VLAN 100 is the native VLAN, so the packet is sent without a VLAN tag.

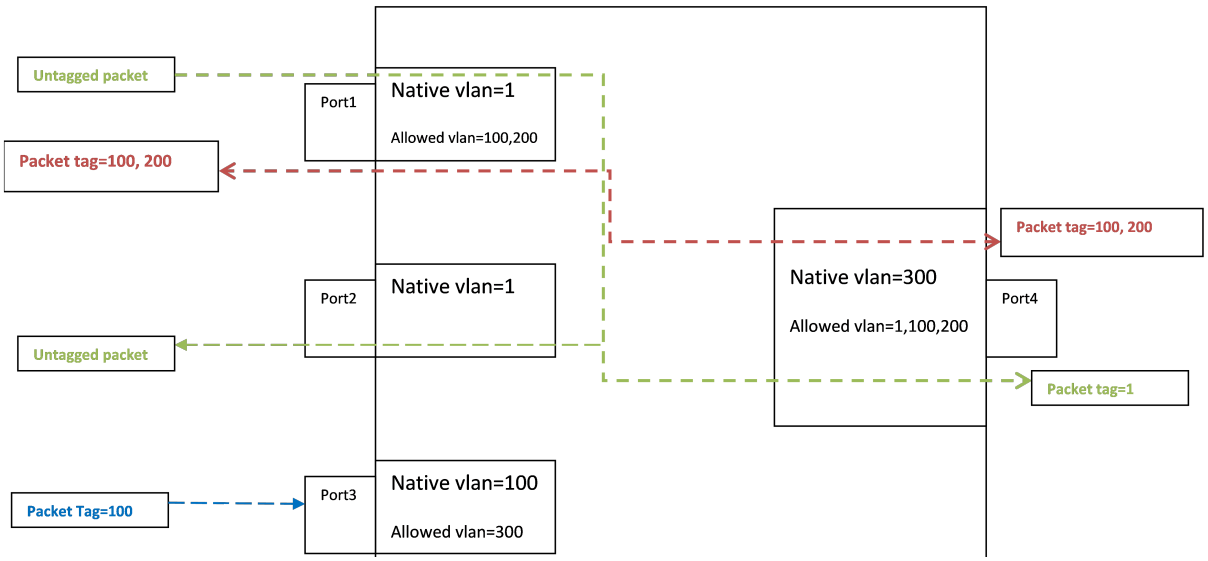
Blue flow:

An untagged packet arriving at Port 4 is assigned VLAN 300 (the native VLAN). Then it flows out all ports that will send Vlan300 (Port 3).

A tagged packet (VLAN 300) arriving at Port3 is allowed. The packet is sent to egress from Port4. VLAN 300 is the native VLAN on Port4, so the packet is sent without a VLAN tag.

Example 2

Example of invalid tagged VLAN.



Green flow:

Between Port1 and Port2, packets are assigned to VLAN 1 at ingress, and then the tag is removed at egress.

Blue flow:

Incoming on Port 3, a tagged packet with VLAN value 100 is allowed, because 100 is the Port 3 native VLAN (the hardware VLAN table accepts a tagged or untagged match to a valid VLAN).

The packet will be sent on port1 and port4 (with packet tag 100).

Spanning Tree Protocol

FortiSwitch supports Spanning Tree Protocol (a link-management protocol that ensures a loop-free Layer 2 network topology) as well as Multiple Spanning Tree Protocol (MSTP), which is defined in the IEEE 802.1Q standard.

MSTP Overview and terminology

MSTP supports multiple spanning tree instances, where each instance carries traffic for one or more VLANs (the mapping of VLANs to instances is configurable).

MSTP is backward-compatible with STP and RSTP. A given Layer 2 network may contain switches that are running MSTP, STP, or RSTP.

MSTP is built on RSTP, so it provides fast recovery from network faults and fast convergence times.

Regions

A region is a set of interconnected switches that have the same MST configuration (region name, MST revision number, and VLAN-to-instance mapping). A network may have any number of regions. Regions are independent of each other (VLAN-to-instance mapping is different in each region).

FortiSwitch supports 15 MST instances in a region. Multiple VLANs can be mapped to each MST instance. Each switch in the region must have the identical mapping of VLANs to instances.

The MST region acts like a single bridge to adjacent MST regions and to non-MST STP protocols.

IST

Instance 0 is a special instance, called the IST. IST is a spanning tree that connects all of the MST switches in a region. All VLANs are assigned to the IST.

IST is the only instance that exchanges BPDUs. The MSTP BPDU contains information for each MSTP instance (captured in an M-record). The M-records are added to the end of a regular RSTP BPDU. This allows MSTP region to inter-operate with an RSTP switch.

CST

The Common Spanning Tree (CST) interconnects the MST regions and all instances of STP or RSTP that are running in the network.

Hop Count and Message Age

MST does not use the BPDU message age within a region. The message-age and maximum-age fields in the BPDU are propagated unchanged within the region.

Within the region, a hop-count mechansim is used to age out the BPDU. The IST root sends out BPDUs with hop count set to Maximum hops. The hop count is decremented each time the BPDU is forwarded. If the hop count reaches zero, the switch discards the BPDU and ages out the information on the receiving port.

STP Port Roles

STP assigns a port role to each switch port. The role is based on configuration, topology, relative position of the port in the topology, and other considerations. Based on the port role, the port either sends or receives STP BPDUs and forwards or blocks the data traffic. Here is a brief summary of each STP port role:

- Designated—One designated port is elected per link (segment). The designated port is the port closest to the root bridge. This port sends BPDUs on the link (segment) and forwards traffic towards the root bridge. In an STP converged network, each designated port is in the STP forwarding state.
- Root—The bridge can have only one root port. The root port is the port that leads to the root bridge. In an STP converged network, the root port is in the STP forwarding state.
- Alternate—Alternate ports lead to the root bridge but are not root ports. The alternate ports maintain the STP blocking state.
- Backup—This is a special case when two or more ports of the same switch are connected together (either directly or through shared media). In this case, one port is designated, and the remaining ports are backup (in the STP blocking state).

STP Loop Protection

The STP loop-protection feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state.

A port remains in blocking state only if it continues to receive BPDU messages. If it stops receving BPDUs (for example, due to unidirectional link failure), the blocking port (alternate or backup port) becomes designated and transitions to a forwarding state. In a redundant topology, this situation may create a loop.

If the loop-protection feature is enabled on a port, that port is forced to remain in blocking state, even if the port stops receiving BPDU messages. It will not transition to forwarding state and does not forward any user traffic.

The loop-protection feature is enabled on a per-port basis. We recommend that you enable loop-protection on all nondesignated ports (all root, alternate, and backup ports).

MSTP configuration

Configuration consists of the following steps:

1. Configure STP settings that are common to all MST instances.
2. Configure settings that are specific to each MST instance.
3. Configure loop-protection on all nondesignated ports.

Configuring STP settings

Some STP settings (region name and MST revision number) are common to all MST instances. Also, protocol timers are common to all instances because only the IST sends out BPDUs.

Using the web-based manager:

1. Go to **Switch** > **STP** > **Settings.**
2. Update the settings as described in the following table.
3. Click **Apply** to save the settings.

Settings	Guidelines
Enable	Enables MSTP for this switch.
Name	Region name. All switches in the MST region must have the identical name.
Revision	The MSTP revision number. All switches in the region must have the same revision number. Range of values is 0 - 65535. Default value is 0.
Hello-Time	Hello time is how often (in seconds) that the switch sends out a BPDU. Range of values is 1 to 10. Default value is 2.
Forward-Time	Forward time is how long (in seconds) a port will spend in the listening-and-learning state before transitioning to forwarding state. Range of values is 4 to 30. Default value is 15.
Max-Age	The maximum age before the switch considers the received BPDU information on a port to be expired. Max-age is used when interworking with switches outside the region. Range of values is 6 to 40. Default value is 20.
Max-Hops	Maximum hops is used inside the MST region. Hop count is decremented each time the BPDU is forwarded. If max-hops reaches zero, the switch discards the BPDU and ages out the information on the receiving port. Range of values is 1 to 40. Default value is 20.

Using the CLI:

```
config switch stp settings
   set forward-time <4 - 30>
   set hello-time <1 - 10>
   set max-age <6 - 40>
   set max-hops <1 - 40>
   set name <region name>
```

```
    set revision <0 - x>
    set status {enable | disable}
end
```

Configuring an MST instance

STP topology is unique for each MST instance in the region. You can configure a different bridge priority and port parameters for each instance.

Using the web-based manager:

1. Go to **Switch** > **STP** > **Instance.**
2. Create a new MST instance or select an existing instance to edit.
3. Update the instance parameters as described in the following table.
4. Click **Apply** to save the settings.

Settings	Guidelines
ID	Instance ID. Range is 1 - 15.
Priority	Priority is a component of bridge ID. The switch with the lowest bridge ID becomes the root switch for this MST instance. Allowed values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.
VLAN Range	The VLANs that map to this MST instance. You can specify individual VLAN numbers or a range of numbers. **NOTE:** Do not assign any VLAN to more than one MST instance. Each VLAN number is in the range 1-4094.
Port Configuration	
Name	Port that will participate in this MST instance.
Cost	The switch uses port cost to select designated ports. Port cost is added to the received PBDU root cost in any BPDU sent on this port. A lower value is preferred. The range of values is 1 to 200,000,000. The default value depends on the interface speed: - 10 Gigabit Ethernet: 2,000 - Gigabit Ethernet: 20,000 - Fast Ethernet: 200,000 - Ethernet: 2,000,000
Priority	The switch uses port priority to choose among ports of the same cost. The port with the lowest priority is put into forwarding state. The valid values are: 0, 32, 64, 96, 128, 160, 192, and 224. The default value is 128.

Using the CLI:

```
config switch stp instance
   edit <instance number>
      set priority <>
      config stp-port
         edit <port name>
            set cost <>
            set priority <>
         next
      set vlan-range <vlan range>
   end
```

Example:

```
config switch stp instance
   edit "1"
      set priority 8192
      config stp-port
         edit "port18"
            set cost 0
            set priority 128
         next
         edit "port19"
            set cost 0
            set priority 128
         next
      end
      set vlan-range 5 7 11-20
   end
```

Configuring STP Port Settings

By default, STP (and edge port) is enabled on all ports.

Configuring STP Edge Port

Use the following commands to enable or disable an interface as an STP edge port:

```
config switch interface
   edit port <number>
      set edge-port <enabled | disabled>
   next
end
```

Configuring STP Loop Protection

By default, STP loop protection is disabled on all ports. Use the following commands to configure STP loop protection on a port:

```
config switch interface
   edit port <number>
      set stp-loop-protection <enabled | disabled>
   next
end
```

Interactions outside of the MSTP Region

A boundary port on an MST switch is a port that receives an STP (version 0) BPDU, an RSTP (version 2) BPDU, or a PBDU from a different MST region.

If the port receives a version 0 BPDU, it will only send version 0 BPDUs on that port. Otherwise, it will send version 3 (MST) BPDUs because the RSTP switch will read this as an RSTP BPDU.

Viewing the MSTP Configuration

To view the MSTP configuration details, use the following commands:

```
get switch stp instance
get switch stp settings
```

Use the following commands to display information about the MSTP instances in the network:

```
diagnose stp instance list
diagnose stp vlan list
diagnose stp mst-config list
```

Link Aggregation Groups

This chapter provides information on how to configure a Link Aggregation Group (LAG). For LAG control, FortiSwitch supports the industry-standard Link Aggregation Control Protocol (LACP). FortiSwitch supports LACP protocol in active and passive modes. In active mode, you can optionally specify the minimum and maximum number of active members in a trunk group.

FortiSwitch supports flap-guard protection for switch ports in a LAG.

Configuring the Trunk and LAG Ports

It is important to configure the trunk to prevent loops.

Using the web-based manager:

1. Go to **Switch > Port > Trunk** and select **Create Trunk**.
2. Give the trunk an appropriate name.
3. Set **Mode** to **static**, **lacp-active**, or **lacp-passive.**
4. Add the required ports to the **Members** list.
5. Select **OK.**

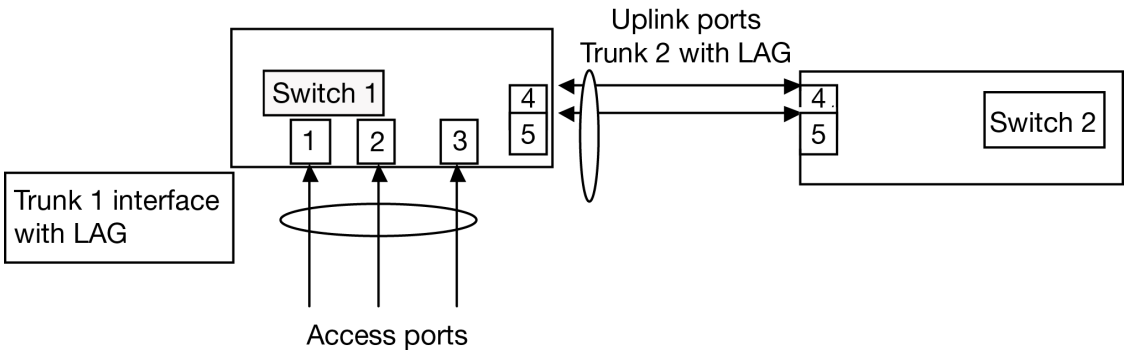
Using the CLI:

```
config switch trunk
   edit <trunk name>
      set description <description_string>
      set members <ports>
      set mode {lacp-active | lacp-passive | static}
      set member-withdrawal-behavior {block | forward}
      set lacp-speed {fast | slow}
      set bundle [enable|disable]
         set min_bundle <integer>
         set max_bundle <integer>
      set port-selection-criteria
          {src-ip | src-mac | dst-ip |dst-mac | src-dst-ip |src-dst-mac}
   end
end
```

Example Configuration

The following is an example CLI configurations for trunk/LAG ports:

Trunk/LAG ports



1. Configure the trunk 1 interface and assign member ports as a LAG group:

```
config switch trunk
   edit trunk1
      set members "port1" "port2" "port3"
      set description test
      set mode lacp-passive
      set port-selection criteria src-dst-ip
   end
end
```

2. Configure the switch ports to have native vlan assignments and allow those vlans on the port that will be the uplink port:

```
config switch interface
   edit port 1
      set native-vlan 1
   next
   edit port 2
      set native-vlan 2
   next
   edit port 3
      set native-vlan 3
   next
   edit port 4
      set native-vlan 4
      set allowed vlans 1 2 3
   next
   edit port 5
      set native-vlan 5
      set allowed-vlans 1 2 3
   end
end
```

3. Configure the trunk 2 interface and assign member ports as a LAG group:

```
config switch trunk
   edit trunk2
```

```
        set members "port4" "port5"
        set description test
        set mode lacp-passive
        set port-selection criteria src-dst-ip
    end
end
```

Viewing the Configured Trunk

To see the details of a configured trunk, use the following command:

```
diagnose switch trunk list
```

MCLAG

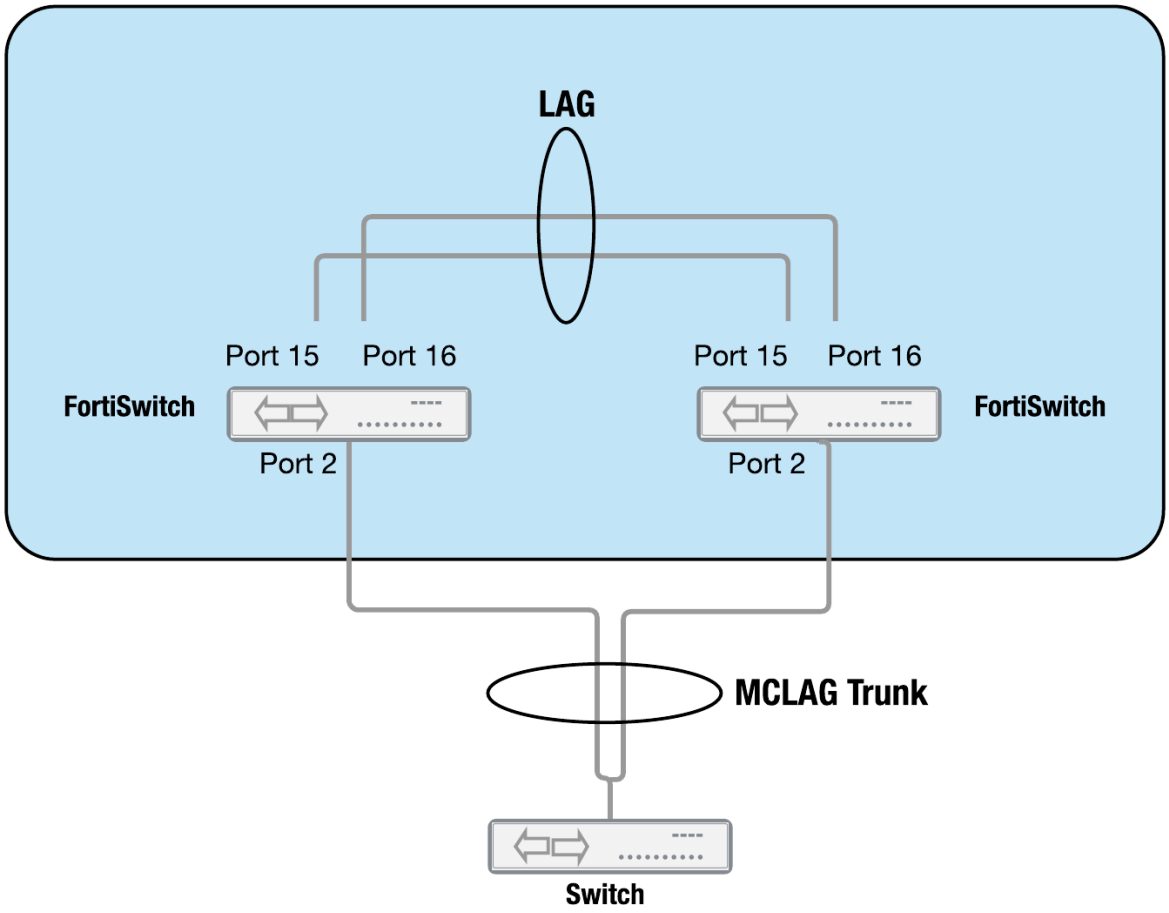
A Link Aggregation Group (LAG) formed by an provides link-level redundancy. A multichassis LAG (MCLAG) provides node-level redundancy by grouping two FortiSwitch models together so that they appear as a single switch on the network. If either switch fails, the MCLAG continues to function without any interruption, increasing network resiliency and eliminating the delays associated with the Spanning Tree Protocol (STP).

Notes

- There is a maximum of two FortiSwitch models per MCLAG.
- The routing feature is not available within a MCLAG.
- For the physical ports of the LAG, the l2-learning feature must be disabled, and the l2-unknown feature must be set to forward.
- Within a MCLAG, STP must be disabled on all ports.
- To use static MAC addresses within a MCLAG, you need to configure MAC addresses on both switches that form the LAG.

Example Configuration

The following is an example CLI configurations for a MCLAG:



1. Create a LAG by configuring the ports for each FortiSwitch:

```
config switch trunk
   edit "LAG-member"
      set mclag-icl enable
      set members "port15" "port16"
   next
end
```

2. Set up the MCLAG:

```
config switch trunk
   edit "first-mclag"
      set mclag enable
      set members "port2"
   next
end
```

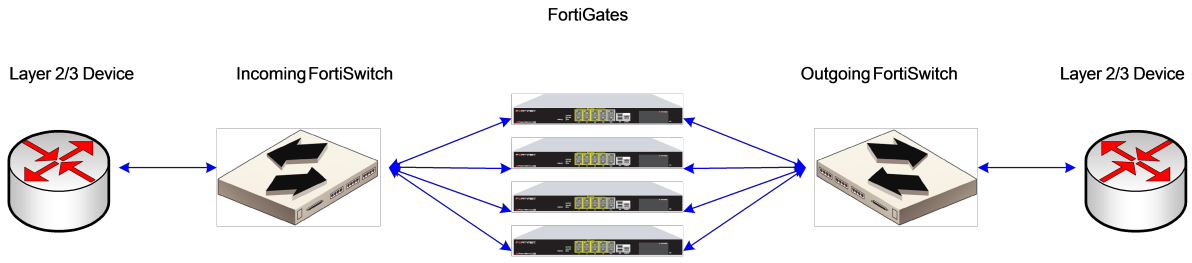
Viewing the Configured Trunk

To see the details of the MCLAG, use the following commands:

```
diagnose switch mclag icl
diagnose switch mclag list
```

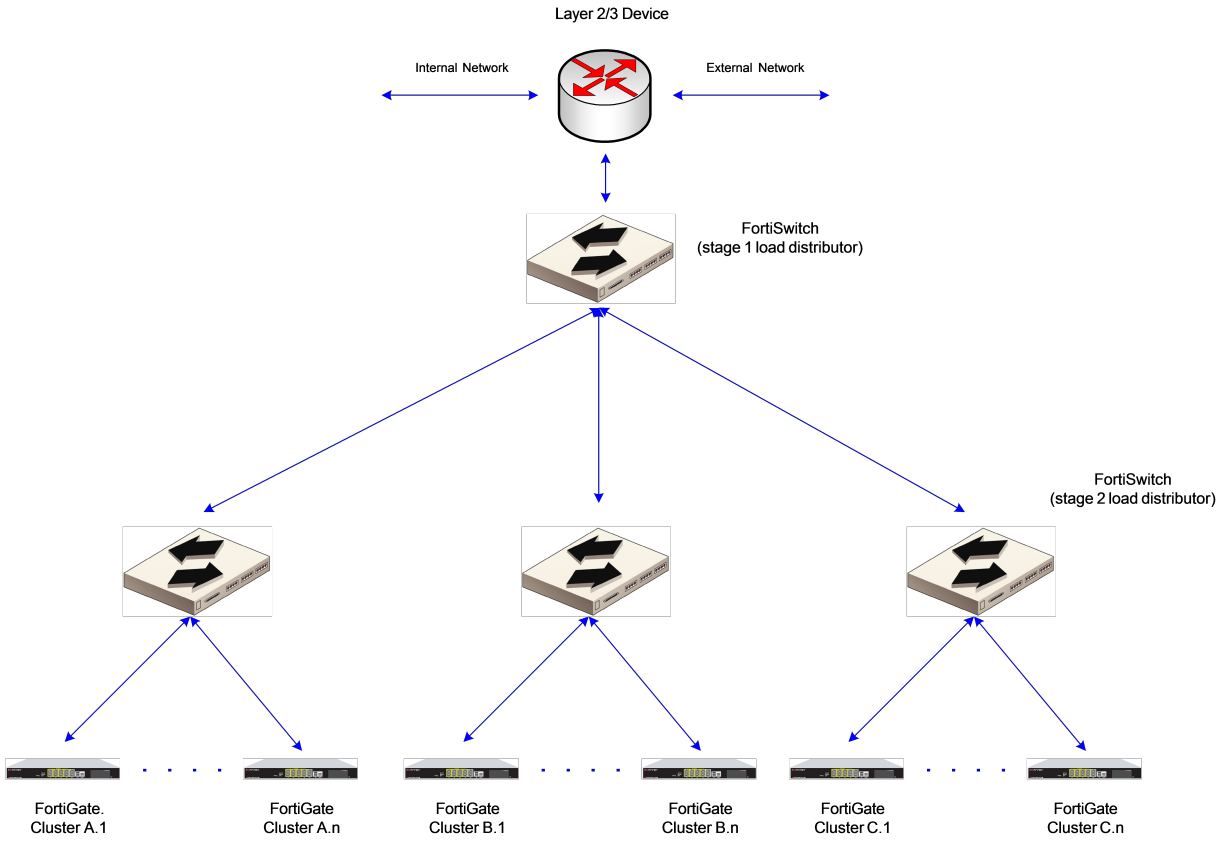
Multi-Stage Load Balance

You can use a FortiSwitch to configure multi-stage load balancing on a set of FortiGate units. This capability allows you to scale security processing while maintaining a simple basic architecture. This configuration is commonly referred to a “firewall sandwich.”



Because FortiGate provides session-aware analysis, the load distribution algorithm must be symmetric (traffic for a given session, in both directions, must all traverse the same FortiGate).

For larger scale deployment, the topology uses multiple layers of load distribution to allow for far larger numbers of FortiGate devices.



The hash at the first and second stages must be symmetric. The two stages must provide different hashing results.

Configuring the Trunk Ports

Use the following commands to configure the trunk members and set the port-selection criteria:

```
config switch trunk
   edit <trunk name>
      set description <description_string>
      set members <ports>
      set mode {fortinet-trunk | lacp-active | lacp-passive | static}
      set port-selection-criteria src-dst-ip-xor16
   end
end
```

Heartbeats

When in fortinet-trunk mode, Heartbeat capability is enabled. Heartbeat messages monitor the status of Fortigate units. If one is unavailable, the FortiSwitch stops sending traffic to that Fortigate until the Fortigate becomes available.

If you enable **hb-verify**, each received heartbeat frame will be validated to match the signature (transmit-port plus switch serial number) and the following configured heartbeat parameters:

- hb-in-vlan
- hb-src-ip
- hb-dst-ip
- hb-src-upd-port
- hb-dst-udp-port

The destination MAC address of the heatbeat frame is set by default to 02:80:c2:00:00:02. You can change the value to any MAC address that is not a broadcast or multicast MAC address.

Configuring Heartbeats

Configure the heartbeat fields using trunk configuration commands, as shown below. By default, all of the configurable values are set to zero, and hb-verify is disabled.

Set the mode to **forti-hb** and set the heartbeat loss limit to a value between 3 and 32.

The heartbeat will transmit at 1-second intervals on any link in the trunk that is up. This value is not configurable.

The heartbeat frame has configurable parameters for the Layer 3 source and destination addresses and the Layer 4 UDP ports. You must also specify the transmit and receive VLANs.

```
config switch trunk
   edit hb-trunk
      set mode fortinet-trunk
      set members <port> [<port>] ... [<port>]
```

```
      set hb-loss-limit <3-32>
      set hb-out-vlan <int>
      set hb-in-vlan <int>
      set hb-src-ip <x.x.x.x>
      set hb-dst-ip <x.x.x.x>
      set hb-src-udp-port <int>
      set hb-dst-udp-port <int>
      set hb-verify [ enable | disable ]
end
```

Use the following command to configure the destination MAC address:

```
config switch global
   set forti-trunk-dmac <mac address>
end
```

Example

The following example creates trunk tr1 with heartbeat capability:

```
config switch trunk
   edit "tr1"
      set mode fortinet-trunk
      set members "port1" "port2"
      set hb-out-vlan 300
      set hb-in-vlan 500
      set hb-src-ip 10.105.7.200
      set hb-dst-ip 10.105.7.199
      set hb-src-udp-port 12345
      set hb-dst-udp-port 54321
      set hb-verify enable
   next
end
```

LLDP-MED

The Fortinet data center switches support LLDP (transmission and reception) wherein the switch will multicast LLDP packets to advertise its identity and capabilities. A switch receives the equivalent information from adjacent Layer 2 peers.

Fortinet data center switches support LLDP-MED (Media Endpoint Discovery), which is an enhancement of LLDP that provides the following facilities:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 priority and differentiated services settings), to enable plug and play networking.
- Device location discovery to allow creation of location databases and Enhanced 911 services for Voice over Internet Protocol (VoIP).
- Extended and automated power management for Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

The switch will multicast LLDP packets to advertise its identity and capabilities. The switch receives the equivalent information from adjacent Layer 2 peers.

Configuration Notes

Fortinet recommends LLDP-MED-capable phones.

The FortiSwitch functions as a Network Connectivity device (that is, NIC, switch, router, and gateway), and will only support sending TLVs intended for Network Connectivity devices.

LLDP supports up to 16 neighbors per physical port.

We accept and parse packets using the CDP (Cisco Discovery Protocol) and count CDP neighbors towards the neighbor limit on a physical port. If neighbors exist, FortiSwitch transmits CDP packets in addition to LLDP.

With release 3.5.1, CDP is independently controllable through **cdp-status** on the physical port. The FortiSwitch no longer requires a neighbor to trigger it to transmit CDP; it will transmit provided cdp-status is configured as tx-only or tx-rx. The default configuration for CDP-status is disabled. It still uses values pulled from the lldp-profile to configure its contents.

LLDP must be globally enabled in switch.lldp.settings for CDP to be transmitted or received:

If a port is added into a *virtual-wire* (connects two ends of a controlled system using a radio frequency [RF] medium), the FortiSwitch will disable transmit and receipt of LLDP and CDP packets and remove all neighbors from the port. This virtual-wire state will be noted in the get switch lldp neighbor-summary output.

If the combination of configured TLVs exceeds the maximum frame size on a port, that frame cannot be sent.

Setting Asset Tag

To help identify the unit, LLDP uses the asset tag, which can be at most 32 characters. It will be added to the LLDP-MED inventory TLV (when that TLV is enabled):

```
config system global
   set asset-tag <string>
end
```

LLDP Global Settings

Using the web-based manager:

1. Go to **Switch > LLDP MED > Settings**.
2. Enable or disable the status.
3. Enter a value for TX hold.
4. Enter the number of seconds for TX interval.
5. Enable or disable the fast start; if you enable fast start, enter the number of seconds.
6. Select the management interface.
7. Click **OK**.

Using the CLI:

```
config switch lldp settings
   set status < enable | disable >
   set tx-hold <int>
   set tx-interval <int>
   set fast-start-interval <int>
   set management-interface <layer 3 interface>
end
```

Variable	Description
status	Enable or disable
tx-hold	Number of tx-intervals before the local LLDP data expires (that is, the packet TTL (in seconds) is **tx-hold** times **tx-interval**). The range for tx-hold is 1 to 16, and the default value is 4.
tx-interval	Frequency of LLDP PDU transmission ranging from 5 to 4095 seconds (default is 30).
fast-start-interval	How often the FortiSwitch transmits the first four LLDP packets when a link comes up. The range is 2 to 5 seconds and the default is 2 seconds. Set this variable to zero to disable fast start.
management-interface	Primary management interface advertised in LLDP and CDP PDUs.

Configuring LLDP Profiles

LLDP profile contains most of the port-specific configuration. Profiles are designed to provide a central point of configuration for LLDP settings that are likely to be the same for multiple ports.

Two static LLDP profiles, **default** and **default-auto-isl**, are created automatically. They can be modified but not deleted. The **default-auto-isl** profile always has auto-isl enabled and rejects any configurations that attempt to disable it.

LLDP-MED network policies

LLDP-MED network policies cannot be deleted or added. To use a policy, set the **med-tlvs** field to include **network-policy** and the desired network policy to **enabled**. The VLAN values on the policy are cross-checked against the VLAN native and untagged attributes for any interfaces that contain physical-ports using this profile. The cross-check determines if the policy Type Length Value (TLV) should be sent (VLAN must be native or allowed) and if the TLV should mark the VLAN as tagged or untagged (VLAN is native, or is in untagged). The network policy TLV is automatically updated when either a switch interface changes VLAN configuration or a physical port is added to, or removed from, a trunk.

FortiSwitch will support the following LLDP-MED TLVs:

- Network Policy TLV
- Inventory Management TLV

Refer to the Configuration Deployment Example at the end of this chapter.

Custom TLVs (Organizationally Specific TLVs)

Custom TLVs, formally known as “Organizationally Specific TLVs” are configured in their own sub-table, available in each profile. They allow you to emulate the TLVs defined in various specifications by using their OUI and subtype and ensuring that the data is formatted correctly. You could also define a purely arbitrary custom TLV for some other vendor or for their company.

The "name" value for each custom TLV is neither used by nor has an effect on LLDP; it simply differentiates config entries:

```
config custom-tlvs
edit <name>
```

The OUI value for each TLV must be set to three bytes. If just one of those bytes is nonzero it is accepted; any value other than "000" is valid. The subtype is optional and ranges from 0 (default) to 255. The information string can be 0 to 507 bytes, in hexadecimal notation.

We do not check for conflicts either between custom TLV values or with standardized TLVs. That is, other than ensuring that the OUI is nonzero, we do not check the OUI, subtype (or data) values entered in the CLI for conflicts with other Custom TLVs or with the OUI and subtypes of TLVs defined by the 802.1, 802.3, LLDP-MED, or other standards. While this behavior could cause LLDP protocol issues, it also allows a large degree of flexibility were you to substitute a standard TLV we do not yet support.

802.1 TLVs

The only 802.1 TLV that can be enabled or disabled is **port-vlan-id**. This TLV will send the native VLAN of the port. This value is updated when the native VLAN of the interface representing the physical port changes or if the physical port is added to, or removed from, a trunk.

By default, no 802.1 TLVs are enabled.

802.3 TLVs

The only 802.3 TLV that can be enabled or disabled is **max-frame-size**. This TLV will send the **max-frame-size** value of the port. If this variable is changed, the sent value will reflect the updated value.

By default, no 802.3 TLVs are enabled.

Auto-isl

The auto-isl configuration that was formerly in the **switch physical-port** CLI has been moved to the **switch lldp-profile** CLI. All behavior and default values are unchanged.

Configuring an LLDP Profile for the Port

Configure an LLDP profile for the port. By default, the port uses the default LLDP profile.

Using the web-based manager:

1. Go to **Switch > LLDP MED > Profile**.
2. Click **Create New**.
3. Enter a name for your LLDP profile.
4. If needed, select port-vlan-id.
5. If needed, select max-frame-size.
6. If needed, enable auto-isl.
7. Enter a value for the auto-isl-hello-timer.
8. Enter a value for the auto-isl-port-group.
9. Enter a value for the auto-isl-receive-timeout.
10. If needed, select inventory-management, network-policy, or both.
11. Click **OK**.

Using the CLI:

```
config switch lldp profile
   edit <profile>
      set 802.1-tlvs port-vlan-id
      set 802.3-tlvs max-frame-size
      set auto-isl {active | inactive}
      set auto-isl-hello-timer <1-30>
      set auto-isl-port-group <0-9>
      set auto-isl-receive-timeout <3-90>
```

```
set med-tlvs (inventory-management | network-policy)
```

Enabling LLDP on a Port

To enable LLDP MED on a port, set the LLDP status to receive-only, transmit-only, or receive and transmit. The default value is tx-rx.

Using the web-based manager:

1. Go to **Switch > Port > Physical**.
2. Select a port and click **Edit**.
3. Select **tx rx**, **rx only**, **tx only**, or **disable**.
4. Select an LLDP profile.
5. Click **OK**.

Using the CLI:

```
config switch physical-port
   edit <port>
      set lldp-status (rx-only | tx-only | tx-rx | disable)
      set lldp-profile <profile name>
   next
end
```

Viewing LLDP Configuration

View the LLDP configuration settings using the web-based manager:

1. Go to **Switch > LLDP MED > Settings**.
2. Click **OK**.

View the LLDP configuration settings using the CLI:

```
get switch lldp settings
status : enable
tx-hold : 4
tx-interval : 30
fast-start-interval : 2
management-interface: internal
```

View the LLDP profiles using the web-based manager:

1. Go to **Switch > LLDP MED > Profile**.
2. Select a profile and click **Edit**.
3. Click **OK**.

View the LLDP profiles using the CLI:

```
get switch lldp profile
== [ default ]
name: default 802.1-tlvs: 802.3-tlvs: med-tlvs: inventory-management network-policy
== [ default-auto-isl ]
name: default-auto-isl 802.1-tlvs: 802.3-tlvs: med-tlvs:
```

Use the following commands to display the LLDP information about LLDP status or the Layer 2 peers for this FortiSwitch:

```
get switch lldp (auto-isl-status | neighbors-detail | neighbors-summary | profile |
    settings | stats)
```

Configuration Deployment Example

Configuring LLDP includes the following steps:

1. Configure LLDP global configuration settings using the **config switch lldp settings** command.
2. Create LLDP profiles using the **config switch lldp profile** command to configure Type Length Values (TLVs) and other per-port settings. (TLVs)
3. Assign LLDP profiles to physical ports.
4. Apply VLAN to interface. (**NOTE:** LLDP profile values that are tied to VLANs will only be sent if the VLAN is assigned on the switch interface.)
   a. Configure profile.

```
show switch lldp profile Forti670i
config switch lldp profile
   edit "Forti670i"
      config med-network-policy
         edit "voice"
            set dscp 46
            set priority 5
            set status enable
            set vlan 400
         next
         edit "guest-voice"
         next
         edit "guest-voice-signaling"
         next
         edit "softphone-voice"
         next
         edit "video-conferencing"
         next
         edit "streaming-video"
            set dscp 40
            set priority 3
            set status enable
            set vlan 400
         next
         edit "video-signalling"
         next
```

```
      end
   set med-tlvs inventory-management network-policy
next
end
```

b. Configure the interface.

```
show switch interface port4
config switch interface
   edit "port4"
      set allowed-vlans 400
      set snmp auto
   next
end
```

c. Connect a phone with LLDP-MED capability to the interface. **NOTE:** Make certain the LLDP, Learning, and DHCP features are enabled.

```
show switch physical-port port4
config switch physical-port
   edit "port4"
      set lldp-profile "Forti670i"
      set speed auto
   next
end
```

d. Verify.

```
show switch lldp neighbor-det port4

Neighbor learned on port port4 by LLDP protocol
Last change 12 seconds ago
Last packet received 12 seconds ago
Chassis ID: 10.105.251.40 (ip)
System Name: FON-670i
System Description:
V12.740.335.12.B
Time To Live: 60 seconds
System Capabilities: BT
Enabled Capabilities: BT
MED type: Communication Device Endpoint (Class III)
MED Capabilities: CP
Management IP Address: 10.105.251.40
Port ID: 00:a8:59:d8:f1:f6 (mac)
Port description: WAN Port 10M/100M/1000M
IEEE802.3, Power via MDI:
Power devicetype: PD
PSE MDI Power: Not Supported
PSE MDI Power Enabled: No
PSE Pair Selection: Can not be controlled
PSE power pairs: Signal
Power class: 1
Power type: 802.3at off
Power source: Unknown
Power priority: Unknown
Power requested: 0
```

```
Power allocated: 0
LLDP-MED, Network Policies:
voice: VLAN: 400 (tagged), Priority: 5 DSCP: 46
voice-signaling: VLAN: 400 (tagged), Priority: 4 DSCP: 35
streaming-video: VLAN: 400 (tagged), Priority: 3 DSCP: 40
```

View LLDP Details

Using the web-based manager:

1. Go to **Switch > Monitor > LLDP**.
2. Select an entry.
3. Click **display detail**.

MAC/IP/Protocol-based VLANs

The FortiSwitch assigns VLANs to packets based on the incoming port or the VLAN tag in the packet. The MAC/IP/Protocol-based VLAN feature enables the assignment of VLANs based on specific fields in an ingress packet (MAC address, IP address, or layer 2 protocol).

Overview

When a MAC/IP/Protocol-based VLAN is assigned to a port, the default behavior is for egress packets with that VLAN value to include the VLAN tag. Use the **set untagged-vlans** port configuration command to remove the VLAN tag from egress packets. For an example of the command, see the Example Configuration.

MAC/IP/Protocol-based VLAN feature assigns the VLAN based on MAC address, IP address, or layer 2 protocol.

MAC Based

In MAC-based VLAN assignment, the FortiSwitch associates a VLAN with each packet based on the originating MAC address.

IP Based

In IP-based VLAN assignment, the FortiSwitch associates a VLAN with each packet based on the originating IP address or IP subnet. IPv4 is supported with prefix masks from 1 to 32. IPv6 is also supported, depending on hardware availability, with prefix lengths from 1 to 64.

Protocol Based

In Protocol-based VLAN assignment, the FortiSwitch associates a VLAN with each packet based on the Ethernet protocol value and the frame type (ethernet2, 802.3d/SNAP, LLC).

Configuring MAC/IP/Protocol-based VLANs

Note the following prerequisites:

1. The VLAN must be created in the FortiSwitch
2. The VLAN needs to be allowed on the ingress port

Using the web-based manager:

1. Go to **Switch** > **VLAN** > **MAC/IP Membership**.
2. Click **Create New** for a new VLAN or select a VLAN and click **Edit**.
3. To configure a MAC-based VLAN:
   a. Click **New** under Member By MAC.
   b. Enter a description and the MAC address.

c. To save the entry, click the plus icon (**+**) to the right of the new entry.

4. To configure an IP-based VLAN:
   a. Click **New** under Member By IPV4.
   b. Enter a description and the IP and Mask.
   c. To save the entry, click the plus icon (**+**) to the right of the new entry.
5. Click **OK**.

Using the CLI:

```
config switch vlan
   edit <vlan-id>
      config member-by-mac
         edit <id>
            set mac XX:XX:XX:XX:XX:XX
            set description <128 byte string>
         next
      end
      config member-by-ipv4
         edit <id>
            set address a.b.c.d/e #subnet mask must 1-32
            set description <128 byte string>
         next
      end
      config member-by-ipv6
         edit <id>
            set prefix xx:xx:xx:xx::/prefix #prefix must 1-64
            set description <128 byte string>
         next
      end
      config member-by-proto
         edit <id>
            set frametypes ethernet2 802.3d llc #default is all
            set protocol 0xXXXX
         next
      end
   next
end
```

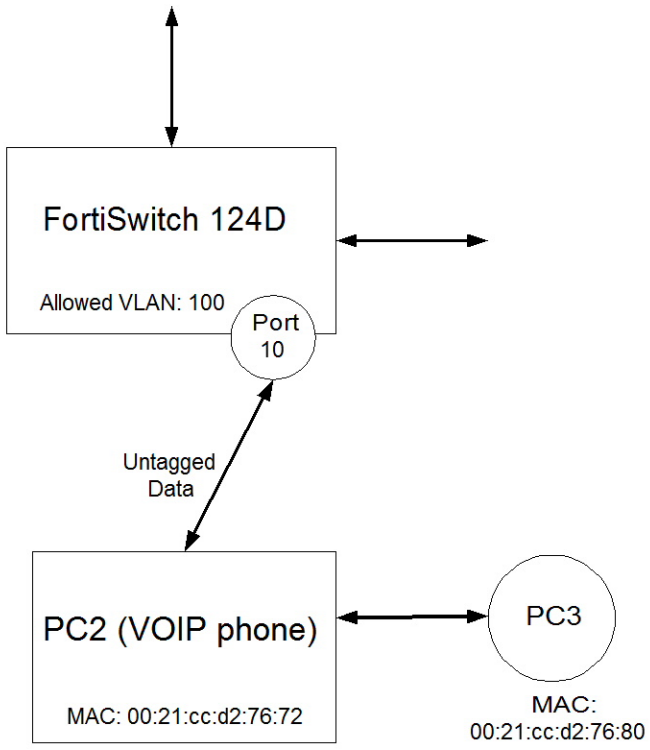
NOTE: There are hardware limits regarding how many MAC/IP/Protocol-based VLANs.you can configure. If you try to add entries beyond the limit, the CLI will reject the configuration:

- editing an existing VLAN - when you enter **next** or **end** on the **config member-by** command
- adding a new VLAN - when you enter **next** or **end** on the **edit vlan** command

Example Configuration

The following example shows a CLI configuration for MAC-based VLAN where a VOIP phone and a PC share the same switch port.

We want to assign a unique VLAN to the voice traffic and leave the PC traffic on the default VLAN for the port.



1. Switch FS-124D Port 10 is connected to PC2 (a VOIP phone), with MAC address 00:21:cc:d2:76:72.
2. The phone also sends traffic from PC3 (MAC= 00:21:cc:d2:76:80).
3. Assign the PC3 traffic to the default VLAN (1) on port 10.
4. Assign the voice traffic to VLAN 100.

Configure the Voice VLAN

```
config switch vlan
   edit 100
      config member-by-mac
         edit 1
            set description "pc2"
            set mac 00:21:cc:d2:76:72
         next
      end
   end
end
```

Configure Switch Port 10

```
config switch interface
   edit "port10"
      # allow vlan=100 on this port
      # treat this as untagged on egress
      set allowed-vlans 100
      set untagged-vlans 100
```

```
      set snmp-index 10
    end
  end
```

Checking the Configuration

To view the MAC-based VLAN assignments, use the following command:

```
diagnose switch vlan assignment mac list sorted-by-mac

 00:21:cc:d2:76:72   VLAN: 100 Installed: yes
Source: Configuration (entry 1)
Description: pc2
```

Mirroring

This chapter contains information on how to configure Layer 2 port mirroring.

Configuring a Mirror

NOTE: You can use virtual wire ports as ingress and egress mirror sources. Egress mirroring of virtual wire ports will have an additional VLAN header on all mirrored traffic.

Using the web-based manager:

1. Go to **Switch** > **Mirror** > **Mirror**.
2. Click **Create New.**
3. Enter a name for the mirror.
4. Set the **Status Enable** check box to set the mirror to active.
5. Select a Destination Port.
6. Select available ports to be used for Ingress Monitoring and Egress Monitoring.
7. Enable the **Packet switching functionality when mirroring** option if the destination port is not a dedicated port. For example, enable this option if you connect a laptop to the switch and you are running a packet sniffer along with the management GUI on the laptop:

Using the CLI:

```
config switch mirror
   edit "m1"
      set dst "port5"
      set src-egress "port2" "port3"
      set src-ingress "port2" "port4"
      set status active
      set switching-packet enable
end
```

Multiple Mirror Destination Ports (MTPs)

With some FortiSwitch models, you can configure multiple mirror destination ports with the following guidelines and restrictions:

- Always set the destination port before setting the src-ingress or src-egress ports.
- Any port configured as a src-ingress or src-egress port in one mirror cannot be configured as a destination port in another mirror.
- For switch models FS-1024D, FS-1048D, and FS--3032D:
  - You can configure a maximum of four mirror destination ports.
  - You can configure a maximum of four ingress/egress ports.
  - The same ingress/egress port can be mirrored to more than one destination port.

- For switch model FSW-124D:
  - You can configure a maximum of four mirror destination ports.
  - Multiple ingress or egress ports can be mirrored to the same destination port.
  - A source ingress port cannot be mirrored to more than one destination port.
  - All source egress ports must be mirrored to the same destination port.
- For switch models FS-108D-POE and FS-224D-POE:
  - You can configure up to seven mirrors, each with a different destination port.
  - There is no limit on the number of ingress or egress ports.
  - An ingress or egress port cannot be mirrored to more than one destination port.

The above restrictions apply to active mirrors. If you try to activate an invalid mirror configuration, the system will display the `Insufficient resources!!` error message.

The following example configuration is valid for FortiSwitch--3032D:

```
config switch mirror
   edit "m1"
      set dst "port16"
      set status active
         set src-ingress "port3" "port5" "port7"
   next
   edit "m2"
      set dst "port22"
      set status active
         set src-ingress "port3" "port5"
   next
   edit "m3"
      set dst "port1"
      set status active
         set src-egress "port3"
   next
   edit "m4"
      set dst "port2"
      set status active
         set src-egress "port3"
end
```

(The above configuration includes three ingress ports, one egress port, and four destination ports. The port3 ingress and egress ports are mirrored to multiple destinations).

The following example configuration is valid for FortiSwitch-224D-POE:

```
config switch mirror
   edit "m1"
      set dst "port1"
      set status active
         set src-ingress "port2" "port7"
   next
   edit "m2"
      set dst "port5"
      set status active
         set src-egress "port2"
   next
   edit "m3"
      set dst "port3"
```

```
        set status active
           set src-ingress "port6"
     next
     edit "m4"
        set dst "port4"
        set status active
           set src-egress "port6" "port8"
end
```

(The above configuration includes three ingress ports, three egress ports and four destination ports. Each ingress and egress port is mirrored to only one destination port).

Access Control Lists

You can use Access Control Lists (ACLs) to configure policies for different types of incoming traffic.

ACL Overview

Key attributes of a policy include:

1. **Interface**. The interface(s) on which traffic arrives at the switch. The interface can be a port, a trunk, or all interfaces. The policy applies to ingress traffic only (not egress traffic).
2. **Classifier**. The classifier identifies the packets that the policy will act on. Each packet can be classified based on one or more criteria. Criteria include source and destination MAC address, VLAN id, source and destination IP address, or service (layer 4 protocol id and port number).
3. **Actions**. If a packet matches the classifier criteria for a given ACL, the following types of action may be applied to the packet:
    - allow or block the packet, redirect the packet, mirror the packet
    - police the traffic
    - mirror the packet to another port, interface or trunk
    - CoS queue assignment
    - outer VLAN tag assignment
    - egress mask to filter packets

The switch uses specialized TCAM memory to perform ACL matching. Each model of FortiSwitch provides different ACL-related capabilities. When you configure the ACL policy, the system will reject the request if the hardware cannot support it.

Configuring ACLs

Major steps to configure an ACL include the following:

1. (Optional) Create or customize a service. FortiSwitch provides a set of pre-configured services that you can use. Use the following command to list the services:
```
show switch acl service custom
```
2. (Optional) Create a policer, if you are defining ACLs to police different types of traffic.
3. Configure the security policies.

Details for each step are as follows:

1. (Optional) Create or customize a service:

```
config switch acl service custom
   edit <service name>
      set comment <string>
      set color
      set protocol {ICMP | IP | TCP/UDP/SCTP}
```

```
      set sctp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-
          <srcporthigh_int>]
      set tcp-portrange <dstportlow_int>[-<dstporthigh_int>:
      <srcportlow_int>-<srcporthigh_int>]
      set udp-portrange <dstportlow_int>[-<dstporthigh_int>:<srcportlow_int>-<srcporthigh_
          int>]
   end
end
```

2. (Optional) Create a policer:

```
config switch acl policer
   edit <policer index>
      set description
      set guaranteed-bandwidth <bandwidth_value>
      set guaranteed-burst <in_bytes>
      set maximum-burst <in_bytes>
```

Each policy is assigned a unique policy ID that is automatically assigned. To view it, use the command **get switch acl policy**.

3. Configure the policy:

```
config switch acl policy
edit <policy-id>
   set description
   set ingress-interface < port >
   set ingress-interface-all {enable | disable}
   config <classifier>
      set src-mac <mac> <mask>
      set dst-mac <mac> <mask>
      set ether-type <integer>
      set src-ip-prefix <IP address> <mask>
      set dest-ip-prefix <IP address> <mask>
      set service <service-id>
      set vlanid <vlan-id>
   end
   config action
      set count {enable | disable}
      set drop {enable | disable}
      set mirror [internal | <port> | <interface> | <trunk>]
      set outer-vlan-tag <integer>
      set policer <policer>
      set redirect [internal | <port>]
      set redirect-bcast-cpu {enable | disable}
      set redirect-bcast-no-cpu {enable | disable}
      set redirect-physical-port <port>
   end
end
```

Configuration Example

Example 1

In the following example, traffic from VLAN 3 is blocked to a specified destination IP subnet (10.10.0.0/16) but allowed to all other destinations:

```
config switch acl policy
   edit 1
      config action
         set count enable
         set drop enable
      end
      config classifier
         set dst-ip-prefix 10.10.0.0 255.255.0.0
         set vlan-id 3
      end
      set ingress-interface-all enable
   next
   edit 2
      config classifier
         set vlan-id 3
      end
      set ingress-interface-all enable
   next
end
```

Example 2

In the following example, Server Message Block (SMB) traffic received on port 1 is mirrored to port 3. SMB protocol uses port 445:

```
config switch acl service custom
   edit "SMB"
      set tcp-portrange 445
   next
end
config switch acl policy # apply policy to port 1 ingress and send to port 3
   edit 1
      set description "cnt_n_mirror_smb"
      set ingress-interface "port1"
      config action
         set count enable
         set mirror "port3"
      end
      config classifier
         set service "SMB"
         set src-ip-prefix 20.20.20.100 255.255.255.255
         set dst-ip-prefix 100.100.100.0 255.255.255.0
      end
   next
end
```

Example 3

FortiSwitch can map different flows (for example, based on source and destination IP addresses) to specific outgoing ports.

In the following example, flows are redirected (based on destination IP) to different outgoing ports, connected to separate FortiDDOS appliances. This allows you to apply different FortiDDOS service profiles to different types of traffic:

```
config switch acl policy # apply policy to port 1 ingress and send to port 3
   edit 1
      config action
         set count enable
         set redirect "port3‟ # use redirect to shift selected traffic to new destination
      end
      config classifier
         set dst-ip-prefix 100.100.100.0 255.255.255.0
      end
      set description "cnt_n_mirror13"
      set ingress-interface "port1"
   next
   edit 2
      config action # apply policy to port 3 ingress and send to port 1
         set count enable
         set redirect "port1"
      end
      config classifier
         set src-ip-prefix 100.100.100.0 255.255.255.0
      end
      set description "cnt_n_mirror31"
      set ingress-interface "port3"
   next
end

config switch acl policy # apply policy to port 1 ingress and send to port 4
   edit 3
      config action
         set count enable
         set redirect "port4‟ # use redirect to shift selected traffic to new destination
      end
      config classifier
         set dst-ip-prefix 20.20.20.0 255.255.255.0
      end
      set description "cnt_n_mirror14"
      set ingress-interface "port1"
   next
   edit 4
      config action # apply policy to port 4 ingress and send to port 1
         set count enable
         set redirect "port1"
      end
      config classifier
         set src-ip-prefix 20.20.20.0 255.255.255.0
      end
      set description "cnt_n_mirror41"
      set ingress-interface "port4"
   next
```

```
end
```

Egress mask

Use the following commands to prevent specific ports from being used for egress:

```
config switch acl policy
   edit <policy-id>
      config classifier
   end
   config action
      set egress-mask <list of physical ports>
   end
end
```

NOTE: The egress-mask command is not supported on dual-chip platforms, such as 448D, 448D-POE, 448D-FPOE, and 248D.

Display commands

Use the following command to display the counters associated with a policy. If you do not provide a policy ID, the system displays all policies that have counters:

```
   get switch acl counters [policy-id]
ID      Packets                 Bytes            description
_____________________________________________________________

0001 1861642              119145728             ip_mac_filter
0100 11160319             714260416             udp_vlan_filter
```

Execute commands

Use the following command to clear the counters associated with a policy. If you do not provide a policy ID, the system clears all of the ACL counters:

```
   execute acl clear-counter <policy-id>
```

Storm Control

Storm control protects a LAN from disruption by traffic storms, which stem from mistakes in network configuration or denial-of-service attacks. A traffic storm, which may consist of broadcast, multicast, or unicast traffic, creates excessive traffic on the LAN and degrades network performance.

By default, storm control is disabled on a FortiSwitch. When enabled, it measures the data rate (in packets-per-second) for unknown unicast, unknown multicast, and broadcast traffic.

You can enable/disable storm control for each of these traffic types individually. If the traffic rate for any of the types exceeds the configured threshold, FortiSwitch drops the excess traffic.

Storm Control configuration is global.

Configuring Storm Control

If you set the rate to zero, the system drops all packets (for the enabled traffic types):

Using the web-based manager:

1. Go to **Switch > Storm Control > Settings**.
2. Enable **Broadcast**, **Unknown Unicast**, and **Unknown Multicast** as required.
3. Enter a value for the rate.
4. Click **Apply** to save the changes.

Using the CLI:

Use the following commands to configure Storm Control:

```
config switch storm-control
   set rate [0 | 1 - 100000]
   set unknown-unicast {enable | disable}
   set unknown-mcast {enable | disable}
   set broadcast {enable | disable}
```

Display commands

Use the following command to display the storm-control configuration:

```
get switch storm-control
```

DHCP Snooping

The DHCP snooping feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. To prevent this, DHCP snooping filters messages on untrusted ports by performing the following activities:

- Validating DHCP messages received from untrusted sources and filters out invalid messages
- Building and maintaining a DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses

Other security features like dynamic ARP inspection (DAI), a security feature that rejects invalid and malicious ARP packets, will also use information stored in the DHCP snooping binding database.

In the FortiSwitch, all ports are untrusted by default. You indicate that a source is trusted by configuring the trust state of its connecting interface.

FortiSwitch supports the option of including Option-82 data in the DHCP request. (DHCP option 82 provides additional security by enabling a controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.)

For the Option-82 Circuit ID field, the following format is used:

Circuit-ID: vlan-mod-port

mod - [(1 Byte) -> Snoop - 1 , Relay - 0]

vlan - [2 bytes]

port - [1 byte]

For the Option-82 Remote ID field, the following format is used:

Remote-ID: mac [6 byte]

Configuring DHCP Snooping

DHCP snooping is enabled per-VLAN and, by default, it is inactive.

Configuring DHCP snooping consists of the following steps:

1. Configure the VLAN settings.
2. Configure the interface settings.

Configure VLAN Settings

Using the web-based manager:

1. Go to **Switch > VLAN > DHCP Snooping**.
2. Click **Create New**.
3. Enter the VLAN identifier.
4. Enter a description for the new VLAN.

5. Enable or disable the private VLAN.
6. If you enabled the private VLAN, enter the number of isolated subVLANs and enter which subVLANS belong to the community, separated by commas.
7. Select the **DHCP Snooping** check box.
8. If needed, select the **Verify Source Mac**, **Insert Option-82**, and **Dynamic ARP Inspection** check boxes.
9. If needed, select the **IGMP Snooping** check box.
10. To enter the MAC addresses that are members, click **New** in the Member By MAC area, enter a description, enter the MAC address, and click **+**.
11. To enter the IPv4 addresses that are members, click **New** in the Member By IPV4 area, enter a description, enter the IPv4 address and mask, and click **+**.
12. Click **OK**.

Using the CLI:

```
config switch vlan
   edit <vlan-id>
      set dhcp-snooping <enable | disable>
      set dhcp-snooping-database <enable | disable>
      set dhcp-snooping-verify-mac <enable | disable>
      set dhcp-snooping-option82 <enable | disable>
   next
end
```

NOTE: If you enable **dhcp-snooping-verify-mac**, the system will verify that the source MAC address in the DHCP request from an untrusted port matches the client hardware address.

NOTE: If you enable **dhcp-snooping-option82**, the system inserts Option-82 data into the DHCP messages for this VLAN.

Configure Interface Settings

After you enable DHCP snooping on a VLAN, all interfaces are in an untrusted state by default. You must explicitly configure the trusted interfaces.

Using the web-based manager:

1. Go to **Switch > Interface > Interface** or **Switch > Interface > Trunk**.
2. Select an interface.
3. Click **Edit**.
4. Select a **Trusted** or **Untrusted** interface for DHCP snooping.
5. If you want to accept DHCP messages with Option-82 data from an untrusted interface, select the **Option-82 Trust** check box.
6. Click **OK**.

Using the CLI:

```
config switch interface / trunk
   edit <interface-name>
      set dhcp-snooping-trust <untrusted | trusted>
      set dhcp-snooping-option82-trust <enable | disable>
   next
end
```

Set **dhcp-snooping-trust** to reflect the trust state of the interface. Where DHCP servers are located, you must configure interfaces as trusted.

If you enable **dhcp-snooping-option82-trust**, the system accepts DHCP messages with Option-82 data from an untrusted interface.

Display Commands

Use the following command to view the detailed status of DHCP snooping VLANs and ports:

```
#get switch dhcp-snooping status

enabled vlans   : 1, 10-15, 500
trusted ports   : port1, port2, port3, trunk_abc
untrusted ports : port4, port5, port6
database        : 75/2048
```

An entry in the DHCP snooping binding database that contains an * after the IP address indicates a temporary or incomplete entry. For example:

```
08:00:27:13:16:51 2000 100.0.0.159* 10 4 port4
```

The DHCP server has not acknowledged this entry yet. If the DHCP server does not acknowledge the entry within 10 seconds, the entry is removed from the database. If the DHCP server does acknowledge the entry within 10 seconds, the entry will be considered “complete” (that is, no * after the IP address), and a proper expiration time is assigned to it.

Use the following command to view the DHCP snooping binding database:

```
#get switch dhcp-snooping database

       mac        vlan     ip     lease(sec) expiry(sec) interface hostname  domainname     vendor
00:01:00:00:00:01 100 xxx.x.x.xxx   86400       86398      port3   host_name domain_name Vendor_String
00:03:00:00:00:03 100 xxx.x.x.x     86400       86394      port5   host_name domain_name Vendor_String
00:03:00:00:00:04 100 xxx.x.x.x     86400       86394      port5   host_name domain_name Vendor_String
```

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) prevents man-in-the-middle attacks and IP address spoofing by checking that packets from untrusted ports have valid IP-MAC-address binding. To use DAI, you must first enable the DHCP snooping feature and then enable DAI for each VLAN. See "DHCP Snooping" on page 92.

Configuring DAI

Configuring DAI consists of the following steps:

1. Enable the violations log. By default, it is enabled.
2. Enable DAI for each VLAN. By default, it is disabled.
3. Enable DAI for the switch interface. By default, all interfaces are in an untrusted state. You must explicitly configure the trusted interfaces.

Enable the Violations Log

```
config switch arp-inspection
   set log-vilolations <enable | disable>
end
```

Enable DAI for Each VLAN

```
config switch vlan
   edit <vlan-id>
      set arp-inspection <enable | disable>
   next
end
```

Enable DAI for the Switch Interface

```
config switch interface
   edit <interface-name>
      set arp-inspection-trust <untrusted | trusted>
   next
end
```

Display Commands

Use the following command to see how many ARP packets have been dropped or forwarded:

```
#diagnose switch arp-inspection status

vlan 100           arp-request               arp-reply
-------------------------------------------------------------------------
received                 0                         0
forwarded                0                         0
dropped                  0                         0
```

IGMP Snooping

FortiSwitch uses the information passed in IGMP messages to optimize the forwarding of multicast traffic.

IGMP snooping allows the FortiSwitch to passively listen to the Internet Group Management Protocol (IGMP) network traffic between hosts and routers. The switch uses this information to determine which ports are interested in receiving each multicast feed. FortiSwitch can reduce unnecessary multicast traffic on the LAN by pruning multicast traffic from links that do not contain a multicast listener.

Essentially, IGMP snooping is a Layer 2 optimization for the Layer 3 IGMP.

The current version of IGMP is version 3, and FortiSwitch is also compatible with IGMPv1 and IGMPv2.

Here is the basic IGMP snooping operation:

1. Host expresses interest in joining a multicast group. (Sends or responds to a join message).
2. FortiSwitch creates an entry in the Layer 2 Forwarding table (or adds the host's port to an existing entry). The switch creates one table entry per VLAN per multicast group.
3. FortiSwitch removes the entry when the last host leaves the group (or when the entry ages out).

Limitations

1. You must enable the IGMP snooping function (using the CLI command **igmp-snooping enable**) before you configure a multicast router port interface.
2. Currently, IGMPv3 (source-specific) is not fully supported. FortiSwitchOS can identify the IGMPv3 query/report messages, but the multicast group creation and traffic replication are based on the multicast group address and VLAN only (IGMPv2 operation).
3. The IGMP snooping entries are added based on multicast group MAC address.
4. Starting with release 3.5.2, the following snooping table limits apply:

Platform Series	IGMP-Snooping Table Limit
124	1024
200	1024
400	1024
500	1024
1024 and 1048	4096
3032	8192

NOTE: Until FSW Release 3.5.1, the table limits were hardware only. The software limit for all platforms was 8192.

Configuring IGMP Snooping

Configuring IGMP snooping consists of the following major steps:

1. Assign VLANs and enable IGMP snooping on the interfaces.
2. Configure IGMP snooping on the VLANs.

NOTE: IGMP snooping configured under "vlan enable" + "port based disable," does not work well; only "vlan level enable" + "port level enable" can make snooping work. So, because the port is "disabled" by default, you must enable IGMP snooping on both the VLAN and the port.

1. Enable IGMP Snooping on the Interfaces

Enable IGMP snooping on a specified switch interface. The default is enabled.

Using the web-based manager:

1. Go to **Switch > Interface > Interface** or **Switch > Interface > Trunk**.
2. Select an interface.
3. Click **Edit**.
4. Select the **IGMP Snooping** check box.
5. If needed, select the **Flood Reports** and **Flood Traffic** check boxes.
6. Click **OK**.

Using the CLI:

```
config switch interface
   edit <port>
      set native-vlan <vlan-id>
      set igmp-snooping (enable | disable)
      set igmps-flood-reports (enable | disable)
   next
end
```

Use the following command to clear the learned/configured multicast group from an interface:

```
execute clear switch igmp-snoop
```

2. Configure IGMP Snooping on the VLANs

Enable IGMP snooping on a specified VLAN interface. The default is disabled.

Using the web-based manager:

1. Go to **Switch > VLAN > IGMP Snooping**.
2. Click **Create New**.
3. Enter the VLAN identifier.
4. Enter a description for the new VLAN.
5. Enable or disable the private VLAN.

6. Select the **IGMP Snooping** check box.
7. Click **OK**.

Using the CLI:

```
config switch vlan
   edit <vlan-id>
      set igmp-snooping [enable |disable]
```

Example:

```
config switch vlan
   edit 30
      set igmp-snooping enable
   next
end
```

Configuration Example

Enable IGMP snooping on the interface ports:

```
config switch interface
   edit port10
      set native-vlan 30
      set igmp-snooping allowed
   next
   edit port2
      set native-vlan 30
      set igmp-snooping allowed
   next
   edit port4
      set native-vlan 30
      set igmp-snooping allowed
   next
   edit port6
      set native-vlan 30
      set igmp-snooping allowed
      next
   edit port8
      set native-vlan 30
      set igmp-snooping allowed
   next
end
```

Configure IGMP snooping on the VLAN:

```
config switch vlan
   edit 30
      set igmp-snooping enable
   end
```

Display Commands

Use the following command to display information about IGMP snooping:

```
# get switch igmp-snooping (globals | group | interface)
```

- **globals**: display the igmp-snooping global configuration on the FortiSwitch
- **group**: display a list of learned groups
- **interface**: display the configured igmp-snooping interfaces and their current state

Display the IGMP snooping global settings

```
FS1D243Z13000023 # get switch igmp-snooping globals
aging-time : 300
flood-unknown-multicast: disabled
```

Display the learned multicast groups

```
FS1D243Z13000023 # get switch igmp-snooping group
Number of Groups: 7
port of-port VLAN GROUP Age
(__port__9) 1 23 231.8.5.4 16
(__port__9) 1 23 231.8.5.5 16
(__port__9) 1 23 231.8.5.6 16
(__port__9) 1 23 231.8.5.7 16
(__port__9) 1 23 231.8.5.8 16
(__port__9) 1 23 231.8.5.9 16
(__port__9) 1 23 231.8.5.10 16
(__port__43) 3 23 querier 17
(__port__14) 8 --- flood-reports ---
(__port__10) 2 --- flood-traffic ---
```

Configuring mRouter ports

Use the following commands to configure a FortiSwitch port as an mRouter port:

NOTE: These settings are not per-VLAN, so the port will act as a querier/mRouter port for all of its associated VLANs.

```
config switch interface
   edit <port>
      set igmp-snooping enable
      set igmps-flood-reports enable
      set igmps-flood-traffic enable
   next
end
```

Private VLANs

A private VLAN (PVLAN) divides the original VLAN (termed the primary VLAN) into sub-VLANs (secondary VLANs), while retaining the existing IP subnet and Layer 3 configuration. Unlike a regular VLAN, which is a single broadcast domain, a PVLAN partitions one broadcast domain into multiple smaller broadcast subdomains.

After a PVLAN VLAN is configured, we use the primary VLAN to forward frames downstream to all secondary VLANs.

There are two main types of secondary VLANs:

- **Isolated**: Any switch ports associated with an isolated VLAN can reach the primary VLAN, but not any other secondary VLAN. In addition, hosts associated with the same isolated VLAN cannot reach each other. Only one isolated VLAN is allowed in one PVLAN domain.
- **Community**: Any switch ports associated with a common community VLAN can communicate with each other and with the primary VLAN but not with any other secondary VLAN. You might have multiple distinct community VLANs within one PVLAN domain.

There are mainly two types of ports in a PVLAN: promiscuous (P-Port) and host.

- **Promiscuous Port (P-Port)**: The switch port connects to a router, firewall, or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port on the VLAN.
- **Host Ports** further divides into two types – isolated port (I-Port) and community port (C-port).
  - **Isolated Port (I-Port)**: Connects to the regular host that resides on isolated VLAN. This port communicates only with P-Ports.
  - **Community Port (C-Port)**: Connects to the regular host that resides on community VLAN. This port communicates with P-Ports and ports on the same community VLAN.

Creating and Enabling a PVLAN

Using the web-based manager:

1. Go to **Switch** > **VLAN** > **PVLAN**.
2. Click **Create New** for a new PVLAN.
3. Enter the VLAN identifier.
4. Enter a description for the new PVLAN.
5. Select **Enable** to enable the new PVLAN.
6. Enter a single VLAN identifier for the isolated sub-VLAN.
7. If needed, enter one VLAN identifier or multiple VLAN identifiers for a common community sub-VLAN.
8. Click **OK**.

Configuring the PVLAN Ports

Using the web-based manager:

1. Go to **Switch** > **Interface** > **Interface**.
2. Select the port to configure.
3. Click **Edit**.
4. Select if the port is a promiscuous port or part of a sub-VLAN.
5. For a promiscuous port, select the primary VLAN identifier.
6. For a port that is part of a sub-VLAN, select the primary VLAN identifier and the sub-VLAN identifier.
7. Click **OK**.

Private VLAN Example

1. Enabling a PVLAN:

```
config switch vlan
   edit 1000
      set private-vlan enable
      set isolated-vlan 101
      set community-vlans 200-210
   end
end
```

2. Configuring the PVLAN ports:

```
config switch interface
   edit "port2"
      set private-vlan promiscuous
      set primary-vlan 1000
   next
   edit "port3"
      set private-vlan sub-vlan
      set primary-vlan 1000
      set sub-vlan 200
   next
   edit "port7"
      set private-vlan sub-vlan
      set primary-vlan 1000
      set sub-vlan 101
   next
   edit "port19"
      set private-vlan promiscuous
      set primary-vlan 1000
   next
   edit "port20"
      set private-vlan sub-vlan
      set primary-vlan 1000
      set sub-vlan 101
   next
   edit "port21"
```

```
        set private-vlan sub-vlan
        set primary-vlan 1000
        set sub-vlan 101
    end
end
```

QoS Settings

Quality of Service (QoS) provides the ability to set particular priorities for different applications, users, or data flows.

QoS involves the following elements:

- **Classification** is the process of determining the priority of a packet. This can be as simple as trusting the QoS markings in the packet header when it is received and so accept the packet. Alternatively, it can hinge on criteria (such as incoming port, VLAN, or service) that are defined by the network administrator.
- **Marking** involves setting fields in the frame or packet header to indicate the priority of this packet. FortiSwitch currently does not support packet marking.
- **Queuing** involves defining priority queues to ensure that packets marked as high priority take precedence over those marked as lower priority. If network congestion becomes so severe that packet drops are inevitable, the queuing process will also select the packets to drop.

Classification

The IEEE 802.1p standard defines a class of service (CoS) value (ranging from 0-7) that is included in the Ethernet frame. The Internet Protocol defines the Layer 3 QoS values that are carried in the IP packet (Differentiated Services, IP Precedence). FortiSwitch provides configurable mappings from CoS or IP-DSCP values to egress queue values.

We recommend that you do not enable trust for both Dot1p and DSCP at the same time on the same interface. If you do wish to trust both Dot1p and IP-DSCP, the switch uses the latter value (DSCP) to determine the queue. The switch will use the Dot1p value and mapping only if the packet contains no DSCP value. For details, refer to the Determining the Egress Queue section below.

Queuing

Queuing determines how queued packets on an egress port will be served. Each egress port supports eight queues, and three scheduling modes are available:

- **Strict Scheduling**: The queues are served in descending order (of queue number), so higher number queues receive higher priority. The purpose of the strict scheduling mode is to provide lower latency service to higher classes of traffic. However, if the interface experiences congestion, the lower priority traffic could be starved.
- **Simple Round Robin (RR)**: In round robin mode, the scheduler visits each backlogged queue, servicing a single packet from each queue before moving on to the next one. The purpose of round robin scheduling is to provide fair access to the egress port bandwidth.
- **Weighted Round Robin (WRR)**: Each of the eight egress queues is assigned a weight value ranging from 0 to 63. The purpose of weighted round robin scheduling is to provide prioritized access to the egress port bandwidth, such that queues with higher weight get more of the bandwidth, but lower priority traffic is not starved.

FortiSwitch QoS Capabilities

FortiSwitch supports the following QoS configuration capabilities:

- Mapping the IEEE 802.1p and Layer 3 QoS values (Differentiated Services and IP Precedence) to an outbound QoS queue number.
- Providing eight egress queues on each port.
- Policing the maximum data rate of egress traffic on the interface.

Determining the Egress Queue

To determine the egress queue value for the packet, we use the configured trust values (and mappings) on the port and the QoS/CoS fields in the packet.

Packets with DSCP and CoS Values

If the port is set to trust DSCP, the switch uses this value to find the queue assignment in the DSCP map for the port.

If the port is set to trust Dot1p and **not** to trust DSCP, the switch uses the packet's CoS value to look up the queue assignment in the Dot1p map for the port

If the port is **not** set to trust Dot1p, the switch uses the default queue 0.

Packets with a CoS Value but No DSCP Value

The switch ignores the trust DSCP value.

1. If the port is set to trust Dot1p, the switch uses the packet's CoS value to look up the queue assignment in the Dot1p map for the port.
2. If the port is **not** set to trust Dot1p, the switch uses the default queue 0.

Packets with a DSCP Value but No CoS Value

If the port is set to trust DSCP, the switch uses the packet's DSCP value to look up the queue assignment in the DSCP map for the port.

If the port is set to trust Dot1p but **not** to trust DSCP, the switch uses the default CoS value of the port to look up the queue assignment in the Dot1p map for the port.

If the port is **not** set to trust Dot1p, the switch uses the default queue 0.

Configuring FortiSwitch QoS

Configure a Dot1p Map

Using the web-based manager:

1. Go to **Switch > QoS > 802.1p config**.
2. Click **Create New**.
3. Enter the name of your Dot1p map.
4. Enter a description of your Dot1p map.
5. Select the queue number for each priority.
6. Click **OK**.

Values that are not explicitly included in the map will follow the default mapping, which maps each priority (0-7) to queue 0. If an incoming packet contains no CoS value, the switch assigns a CoS value of zero.

Using the CLI:

To configure a Dot1p map, which defines a mapping between IEEE 802.1p CoS values (from incoming packets on a trusted interface) and the egress queue values, enter the following:

```
config switch qos dot1p-map
   edit <dot1p map name>
      set description <text>
      set [priority-0|priority-1|priority-2|....priority-7] <queue number>
   next
end
```

Example:

```
config switch qos dot1p-map
   edit "test1"
      set priority-0 queue-2
      set priority-1 queue-0
      set priority-2 queue-1
      set priority-3 queue-3
      set priority-4 queue-4
      set priority-5 queue-5
      set priority-6 queue-6
      set priority-7 queue-7
   next
   end
```

Values that are not explicitly included in the map will follow the default mapping, which maps each priority (0-7) to queue 0. If an incoming packet contains no CoS value, the switch assigns a CoS value of zero.

Use the **set default-cos** port command to set a different default CoS value, ranging from 0 to 7:

```
config switch interface
   edit port1
      set default-cos <0-7>
```

Configure a DSCP Map

A DSCP map defines a mapping between IP precedence or DSCP values and the egress queue values.

Using the web-based manager:

1. Go to **Switch > QoS > IP precedence/DSCP**.
2. Click **Create New**.
3. Enter the name of your DCSP map.
4. Enter a description of your DCSP map.
5. Select which queue to configure.
6. Select the differentiated services to use.
7. Select the IP precedence to use.
8. Enter the raw values to use.
9. Click **OK**.

Using the CLI:

```
config switch qos ip-dscp-map
   edit <ip-dscp map name>
      set description <text>
      config map
      edit <entry-name1>
         set diffserv [ [ AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 |
             AF41 | AF42 | AF43 | CS0 | CS1 | CS2 | CS3 | CS4 | CS5 | CS6 | CS7 | EF ]
         set ip-precedence [ Network Control | Internetwork Control | Critic/ECP | Flash
             Override | Flash, Immediate | Priority | Routine ]
         set value <dscp raw value>
         set cos-queue <queue number>
      next
   end
end
```

The following example defines a mapping for two of the DSCP values:

```
config switch qos ip-dscp-map
   edit "m1"
      config map
         edit "e1"
            set cos-queue 0
            set ip-precedence Immediate
         next
         edit "e2"
            set cos-queue 3
            set value 13
         next
      end
   next
end
```

Configure Egress QoS Policy

In a QoS policy, you set the scheduling mode (Strict, Round Robin, or Weighted Round Robin) for the policy, and configure one or more CoS queues.

A valid set of values include the following:

- min-rate: minimum rate in kbps
- max-rate: maximum rate in kbps
- drop policy: taildrop or random early detection
- weight value (applicable if the policy schedule is weighted)

Using the web-based manager:

1. Go to **Switch > QoS > Egress Policy**.
2. Click **Create New**.
3. Enter the name of your QoS egress policy.
4. Select the scheduling mode to use.
5. For each queue, enter a description and select the drop policy to use.
6. For each queue, enter the minimum rate in kbps, maximum rate in kbps, and weight value.
7. Click **OK**.

Using the CLI:

```
config switch qos qos-policy
   edit < policy.name >
      set schedule [ strict | round-robin | weighted ]
      config cos-queue
      edit [queue0 ... queue7]
         set description <text>
         set min-rate <rate kbps>
         set max-rate <rate kbps>
         set drop-policy {taildrop | random-early-detection | weighted-random-early-
             detction}
         set weight <value>
      end
   next
end
```

Configure Egress Drop Mode

NOTE: The egress-drop-mode command is available only for the 1024/1048/3032/5xx series.

When there are too many packets going through the same egress port, you can choose whether packets are dropped on ingress or egress.

Use the following commands to set the drop mode:

```
config switch physical-port
   edit <port>
      set egress-dop-mode <disabled | enabled>
   end
```

Variable	Description
disabled	Drop packets on ingress.
enabled	Drop packets on egress.

NOTE: Because too many packets are going through the same egress port, you might want to use the pause frame for flow control on the ingress side. To see the pause frame on ingress, enable the flow control “tx” on the ingress interface and disable egress-drop-mode on the egress interface.

Configure Switch Ports

You can configure the following QoS settings on a switch port or a trunk:

- trust dot1p values on ingress traffic and the dot1p map to use
- trust ip-dscp values on ingress traffic and the ip-dscp map to use. (**Note:** Trust the dot1p values **or** the ip-dscp values but not both.)
- an egress policy for the interface
- a default CoS value (for packets with no CoS value)

If neither of the trust policies is configured on a port, the ingress traffic is mapped to queue 0 on the egress port.

If no egress policy is configured on a port, we apply the default scheduling mode (that is, round-robin).

Using the web-based manager:

1. Go to **Switch > Interface > Interface**.
2. Select the switch port to update and click **Edit**.
3. Select the QoS egress policy.
4. Select the Dot1p map.
5. Select the DSCP map.
6. Click **OK**.

Example:

```
config switch interface
   edit <port>
      set trust-dot1p-policy <map-name>
      set trust-ip-dscp-policy <map-name>
      set qos-policy < policy-name >
      set default-cos <default cos value 0-7>
   next
end
```

Configure QoS on Trunks

Configuring QoS on trunk interface follows the same configuration steps as for a switch port (configure a Dot1p/DSCP map and an egress policy).

When you add a port to a trunk, the port inherits the QoS configuration of the trunk interface. A port member will revert to the default QoS configuration when it is removed from the trunk interface.

Using the web-based manager:

1. Go to **Switch > Interface > Trunk**.
2. Select the trunk to update and click **Edit**.
3. Select the QoS egress policy.
4. Select the Dot1p map.
5. Select the DSCP map.
6. Click **OK**.

The following example shows QoS configuration on a trunk interface:

```
config switch interface
   edit "tr1"
      set snmp-index 56
      set trust-dot1p-map "dot1p_map1"
      set default-cos 1
      set qos-policy "p1"
   next
end
```

When you configure an egress qos policy with rate control on a trunk interface, that rate control value is applied to each port in the trunk interface. The FortiSwitch does not support an aggregate value for the whole trunk interface.

Configure QoS on VLANs

You can configure a CoS queue value for a VLAN by creating an ACL policy:

```
config switch acl policy
   edit 1
      config action
         set cos-queue 7
         set count enable
      end
      config classifier
         set vlan-id 200
      end
      set ingress-interface "port25"
end
```

sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that may impact performance and throughput. With sFlow you can export truncated packets and interface counters. FortiSwitch implements sFlow version 5 and supports trunks and VLANs.

About sFlow

sFlow uses packet sampling to monitor network traffic. The sFlow agent captures packet information at defined intervals and sends them to an sFlow collector for analysis, providing real-time data analysis. To minimize the impact on network throughput, the information sent is only a sampling of the data.

The sFlow collector is a central server running software that analyzes and reports on network traffic. The sampled packets and counter information, referred to as flow samples and counter samples, respectively, are sent as sFlow datagrams to a collector. Upon receiving the datagrams, the sFlow collector provides real-time analysis and graphing to indicate the source of potential traffic issues. sFlow collector software is available from a number of third-party software vendors.

Configuring sFlow

Configuration consists of the following steps:

1. Enable the sFlow Agent.
2. Configure sampling information on the interfaces.

Configure sFlow Agents

Use the following commands to configure an sFlow agent:

1. Set the IP address of the collector.
2. Set the collector port number, which is the destination port number in sFlow UDP packets. The default value is 6343.

Using the web-based manager:

1. Go to **System > Network > sFlow**.
2. Set the collector IP address and port number.
3. Click **OK** to save the changes.

Using the CLI:

```
config system sflow
   set collector-ip <ip/hostname>
   set collector-port <port>
```

Configure the Interfaces

Use the following commands to configure sFlow on a port:

- Enable sFlow on the port (by default, sFlow is disabled).
- Set the sample rate. An average of one out of **count** packets is randomly sampled. The rate ranges from 0-99999; the default is 512.
- Set the direction for capturing the traffic. sFlow can capture the ingress traffic (RX), the egress traffic (TX), or both (the default).
- Set the polling interval, which defines how often the switch sends interface counters to the collector. The range of values is 1-255 and default is 30.

Using the web-based manager:

1. Go to **Switch > Interface > Interface.**
2. Select one or more ports to update and click **Edit**.
3. If you selected more than one port, the port names are displayed in the name field, separated by commas.
4. Set **Enable sFlow**.
5. Enter new values as required for Sample Rate, Sample Direction, and Polling Interval.
6. Click **OK** to save the changes.

Using the CLI:

```
config switch interface
   edit <port>
      set sflow-sampler [enabled | disabled]
      set sample-rate <count>
      set sample-direction [rx | tx | both]
      set polling-interval <interval>
```

NOTE: Ensure that you can use the exec command `ping collector_ip_address` to ping the collector from the FortiSwitch. Then, use the built-in sniffer to trace sFlow packets (`diag sniff packet <vlan_interface_name> "udp port 6343"`).

Display commands

Use the following command to display the sFlow configuration:

```
get system sflow
```

Feature Licensing

Advanced features (such as dynamic routing protocols) require a feature license.

About Licenses

Each feature license is tied to the serial number of the FortiSwitch. Therefore, a feature license is valid on one system.

Configuring Licenses

Configuration consists of the following steps:

1. Check license status.
2. Add a license.

Checking license status

Using the web-based manager:

1. Go to **System > Dashboard > Status**.
2. Check which licenses that are currently active.

Using the CLI:

```
execute license status
```

Adding a license

Using the web-based manager:

1. Go to **System > Config > License**.
2. Click **Add**.
3. Enter your license key.
4. Click **OK**.

NOTE: Adding license keys causes the system to log you out.

Using the CLI:

```
execute license add <key>
```

Removing a license

Using the web-based manager:

1. Go to **System > Config > License**.
2. Select a license to remove
3. Click **Delete**.
4. Click **OK** to acknowledge the warning.

NOTE: Deleting license keys causes the system to log you out before rebooting. You will lose all configurations related to the license.

Using the CLI:

```
execute license type <type> clear
```

Layer 3 Interfaces

Fortinet data center switches support loopback interfaces and Switched Virtual Interfaces (SVIs), both of which are described in this section.

Loopback Interfaces

A loopback interface is a special virtual interface created in software that is not associated with any hardware interface.

Dynamic routing protocols typically use a loopback interface as a reliable IP interface for routing updates. You can assign the loopback IP address to the router rather than the IP address of a specific hardware interface. Services (such as Telnet) can access the router using the loopback IP address, which remains available independent of hardware interfaces status.

No limit exists on the number of loopback interfaces you can create.

A loopback interface does not have an internal VLAN ID or a MAC addresses and always uses a /32 network mask.

Configuring Loopback Interfaces

Using the web-based manager:

1. Go to **System > Network > Interface** and select **Create New**.

Using the CLI:

```
config system interface
   edit "loopback"
      set ip 172.168.20.1 255.255.255.255
      set allowaccess ping https http ssh telnet
      set type loopback
      set snmp-index 28
   next
end
```

Switched Virtual Interfaces

A Switched Virtual Interface (or SVI) is a logical interface that is associated with a VLAN and supports routing and switching protocols.

You can assign an IP address to the SVI to enable routing between VLANs. For example, we may use SVIs to route between two different VLANs connected to a switch (no need to connect through a Layer 3 router).

Configuring a Switched Virtual Interface

Using the web-based manager:

1. Go to **System > Network > Interface** and select **Create New**.
2. Provide the interface an appropriate name.
3. Set **Interface** to **internal**.
4. Set a **VLAN ID**.
5. Assign an **IP/Netmask**.
6. Set **Administrative Access** to allow ping, SSH, and Telnet.
7. Select **OK**.

Using the CLI:

Create a system interface. Give it an IP subnet and an associated VLAN:

```
config system interface
   edit <system interface name>
      set ip <IP address and mask>
      set vlanid <vlan>
      set allowacess ping ssh telnet
```

Example SVI Configuration

The following is an example CLI configuration for SVI static routing.

In this configuration, Server-1 is connected to switch Port1, and Server-2 is connected to switch Port2. Port1 is a member of VLAN 4000, and Port2 is a member of VLAN 2. Port1 is the gateway for Server-1, and port2 is the gateway for Server-2.

(**NOTE:** For simplicity, assume that both port1 and port are on same switch.)

1. Configure the native VLANs for Port 1 and Port 2:

```
config switch interface
   edit port1
      set native-vlan 4000
   edit port2
      set native-vlan 2
   end
```

2. Create L3 system interfaces that correspond to Port 1 (VLAN 4000) and Port 2 (VLAN 2):

```
config system interface
   edit vlan4000
      set ip 192.168.11.1/24
      set vlanid 4000
      set allowacess ping ssh telnet
   next
      edit vlan2
         set ip 192.168.10.1/24
         set vlanid 2
         set allowacess ping ssh telnet
   end
```

Viewing SVI Configuration

Display the status of SVI configuration using following command:

```
show system interface [ <sytem interface name> ]
```

Layer 3 Routing in Hardware

In Release 3.3.0 and later, some FortiSwitch models support hardware-based Layer 3 forwarding.

For FortiSwitch models that support Equal Cost Multi-Path (ECMP) (see the feature matrix in Introduction), forwarding for all ECMP routes is performed in hardware.

For switch models that support hardware-based Layer 3 forwarding but do not support ECMP, only one route to each destination will be hardware-forwarded. If you configure multiple routes to the same destination, you can configure a priority value for each route. Only the route with highest priority will be forwarded by the hardware. If no priority values are assigned to the routes, the most recently configured route will be forwarded by the hardware.

Router Activity

Logging allows you to review all router activity.

NOTE: Router logs are available only on supported platforms if you have the advanced features license.

To enable router logging:

1. Go to **Log > Log Config > Log Setting**.
2. Select **Event Logging**.
3. Select **Router activity event**.
4. Select **Apply**.

To view router logs:

1. Go to **Log > Log Config > Event Log > Router**.
2. Click **Download Raw Log** if you want to review the entries offline.

Equal Cost Multi-Path (ECMP) Routing

ECMP is a forwarding mechanism that enables load-sharing of traffic to multiple paths of equal cost. An ECMP set is formed when the routing table contains multiple next-hop address for the same destination with equal cost. Routes of equal cost have the same preference and metric value. If there is an ECMP set for an active route, the switch uses a hash algorithm to choose one of the next-hop addresses. As input to the hash, the switch uses one or more of the following fields in the packet to be routed:

- Source IP
- Destination IP
- Input Port

Configuring ECMP

The switch will automatically use ECMP to choose between equal-cost routes.

This configuration value is system-wide. Source IP is the default value.

Notes and Restrictions

When you configure a static route with a gateway, the gateway must be in the same IP subnet as the device. Also, the destination subnet cannot match any of device IP subnets in the switch.

When you configure a static route without a gateway, the destination subnet must be in the same IP subnet as the device.

Using the CLI:

```
config system settings
   set v4-ecmp-mode [ source-ip-based ] [ dst-ip-based ] [ port-based ]
end
```

Example ECMP Configuration

The following is an example CLI configuration for ECMP forwarding.

In this configuration, we configure Port2 and Port6 as routed ports. We create interfaces I-RED and I-GREEN as RVI interface. The remaining ports in the switch are normal Layer 2 ports.

1. Configure Native VLANs for Port2, Port6, and Port9. Also configure the “internal” interface to allow native VLANs for Port2, Port6, and Port9:

```
config switch interface
   edit port2
      set native-vlan 10
   edit port6
      set native-vlan 20
   edit port9
      set native-vlan 30
   edit internal
      set allowed-vlans 10,20,30
   end
```

2. Configure system interfaces:

```
config system interface
   edit "internal"
      set type physical
   next
      edit "i-blue"
         set ip 1.1.1.1 255.255.255.0
         set allowaccess ping https http ssh snmp telnet
         set vlanid 10
         set interface internal
   next
      edit "i-red"
         set ip 172.16.11.1 255.255.255.0
         set allowaccess ping ssh telnet
         set vlanid 20
         set interface internal
```

```
    next
       edit "i-green"
          set ip 172.168.13.1 255.255.255.0
          set allowaccess ping https http ssh snmp telnet
          set vlanid 30
          set interface internal
    next
end
```

3. Configure static routes. Here, we are configuring multiple next hop gateway for the same network:

```
config router static
   edit 1
      set device "mgmt"
      set gateway 10.105.0.1
   next
   edit 2
      set device "i-red"
      set dst 8.8.8.0/24
      set gateway 172.16.11.2
   next
   edit 3
      set device "i-green"
      set dst 8.8.8.0/24
      set gateway 172.168.13.2
   next
```

Viewing ECMP Configuration

Display the status of the ECMP configuration using following command:

```
show system interface [ <sytem interface name> ]
```

Bidirectional Forwarding Detection

Starting in FortiSwitchOS v3.4.2, we supported Static Bidirectional Forwarding Detection (BFD), a point-to-point protocol to detect faults in the datapath between the endpoints of an IETF-defined tunnel (such as IP, IP-in-IP, GRE, and MPLS LSP/PW).

BFD defines Demand mode and Asynchronous mode operation. The FortiSwitch supports Asynchronous mode. In this mode, the systems periodically send BFD Control packets to one another, and if a number of those packets in a row are not received by the other system, the session is declared to be down.

BFD packets are transported using UDP/IP encapsulation and BFD control packets are identified using well-known UDP destination port 3784 (**NOTE:** BFD echo packets are identified using 3785).

BFD packets are not visible to the intermediate nodes and are generated and processed by the tunnel end systems only.

Configuring BFD

Use the following steps to configure BFD:

1. Configure the following values in the system interface:
   - **Enable BFD**: Set to **enable**, or set to **global** to inherit the global configuration value.
   - **Desired min TX interval**: This is the minimum interval that the local system would like to use between transmission of BFD control packets. Value range is 200 ms – 30,000 ms. Default value is 250.
   - **Required min RX interval**: This is the minimum interval that the local system can support between receipt of BFD control packets. If you set this value to zero, the remote system will not transmit BFD control packets. The value range is 200 ms – 30000 ms. The default value is 250.
   - **Detect multi**: This is the detection time multiplier. The negotiated transmit interval multiplied by this value is the Detection Time for the receiving system. The value range is 1 – 20. The default is 3.
2. Enable BFD in the static router configuration.

Using the CLI:

```
config system interface
   edit <system interface name>
      set bfd [enable| disable | global]
      set bfd-desired-min-tx <number of ms>
      set bfd-required-min-rx <number of ms>
      set bfd-detect-multi [1…20]
next
config router static
edit 1
   set bfd enable
```

Viewing BFD Configuration

Display the status of BFD sessions using following command:

```
get router info bfd neighbor [ <IP address of neighbor>]
```

```
OurAddr          NeighAddr        LD/RD    State    Int
192.168.15.2     192.168.15.1     1/4      UP       vlan2000
192.168.16.2     192.168.16.1     2/2      UP       vlan2001
```

Use the following command to display additional details:

```
get router info bfd neighbor detail
```

IP-MAC Binding

Use IP-MAC binding to prevent ARP spoofing.

The port accepts a packet only if the source IP address and source MAC address in the packet match an entry in the IP-MAC binding table.

You can enable/disable IP-MAC binding for the whole switch, and you can override this global setting for each port.

Configuring IP-MAC Binding

Use the following steps to configure IP-MAC binding:

1. Enable the IP-MAC binding global setting.
2. Create the IP-MAC bindings. You can activate each binding individually.
3. Set each port to follow the global setting. You can also override the global setting for individual ports by enabling or disabling IP-MAC binding for the port.

Using the web-based manager:

Enable the IP-MAC binding global setting:

1. Go to **Switch** > **IP MAC Binding** > **Settings**.
2. Click **Enable** to enable IP-MAC binding.
3. Click **Apply** to save the change.

Create the IP-MAC bindings:

1. Go to **Switch** > **IP MAC Binding** > **Bindings**.
2. Click **Create New** to create a new binding.

Enable IP-MAC binding on the interface:

1. Go to **Switch** > **Interfaces** > **Interface**.
2. Edit the interface to be configured.
3. Select one of the IP-MAC binding settings.

Using the CLI:

```
config switch global
   set ip-mac-binding [enable| disable]

config switch ip-mac-binding
   edit 1
      set ip <IP address and network mask>
      set mac <MAC address>
      set status (enable| disable)
   next
end
config switch interface
   edit <port>
      set ip-mac-binding (enable| disable | global)
   edit <trunk name>
      set ip-mac-binding (enable| disable | global)
```

Notes

For a switch port, the default IP-MAC binding value is disabled.

When you configure a trunk, the trunk follows the global value by default. You can also explicitly enable or disable IP-MAC binding for a trunk, as shown above.

When you add member ports to the trunk, all ports take on the trunk setting. If you later remove a port from the trunk group, the port is reset to the default value (disabled).

No duplicate entries are allowed in the mapping table.

Rules are disabled by default. You need to explicitly enable each rule.

The mapping table holds up to 1024 rules.

Viewing IP-MAC Binding Configuration

Display the status of IP-MAC binding using the following command:

```
show switch ip-mac-binding <entry number>
```

DHCP Relay

DHCP clients send broadcast requests to a DHCP server. Without DHCP relay, the DHCP client and server must be on the same subnet. DHCP relay behaves as a proxy between DHCP clients and a DHCP server on a different subnet.

When the DHCP relay receives a DHCP request from a host on an inside interface, it forwards the request to one of the specified DHCP servers on an outside interface. When the DHCP server responds to the client request, the DHCP relay forwards the response back to DHCP client.

Detailed Operation

DHCP relay operates as follows:

1. DHCP client C broadcasts a DHCP/BOOTP discover message on its subnet.
2. The relay agent examines the gateway IP address field in the DHCP/BOOTP message header. If the field has an IP address of 0.0.0.0, the agent fills it with the relay agent's or router's IP address and forwards the message to the remote subnet of the DHCP server.
3. When DHCP server receives the message, it examines the gateway IP address field for a DHCP scope that can be used by the DHCP server to supply an IP address lease.
4. If DHCP server has multiple DHCP scopes, the address in the gateway IP address field (GIADDR) identifies the DHCP scope from which to offer an IP address lease.
5. DHCP server sends an IP address lease offer (DHCPOFFER) directly to the relay agent identified in the gateway IP address (GIADDR) field.
6. The router then relays the address lease offer (DHCPOFFER) to the DHCP client.

Notes

DHCP relay service supports up to 8 relay targets per interface.

Each target is sent a copy of the DHCP message.

Configuring DHCP Relay

You can configure DHCP relay on any Layer 3 interface.

Using the web-based manager:

1. Go to **System > Network > Interface**.
2. Select an interface.
3. Click **Edit**.
4. Select the **DHCP Relay** check box.

5. Enter the IP addresses for the relay servers, separated by a space.
6. If you want to include Option-82 data, select the **Option-82** check box.
7. Click **OK**.

Using the CLI:

```
config system interface
   edit <interface-name>
      set dhcp-relay-service (enable | disable)
      set dhcp-relay-ip <ip-address1> [<ip-address2> ... <ip-address8>]
      set dhcp-relay-option82 (enable | disable)
   next
end
```

Configuration Example

In the following example, the DHCP server has address 192.168.23.2:

```
edit "v15-p15"
  set dhcp-relay-service enable
  set dhcp-relay-ip "192.168.23.2"    -> the DHCP server address
  set ip 192.168.15.1 255.255.255.0   -> the DHCP client subnet
  set allowaccess ping ssh snmp telnet
  set snmp-index 53
  set vlanid 15
  set interface "internal"
end
```

OSPF Routing

NOTE: You must have an advanced features license to use OSPF routing.

OSPF (Open Shortest Path First) is a link-state interior routing protocol that is widely used in large enterprise organizations. OSPF provides routing within a single autonomous system (AS). This differs from BGP, which provides routing between autonomous systems.

An OSPF autonomous system (AS) may contain only one area, or it may consist of a group of areas connected to a backbone area. A router connected to more than one area is an area border router (ABR). Routing information is contained in a link state database. Routing information is communicated between routers using link state advertisements (LSAs).

The main benefit of OSPF is that it detects link failures in the network quickly and converges network traffic successfully within seconds without any network loops. Also, OSPF has features to control which routes are propagated to contain the size of the routing tables.

You can enable Bidirectional Forwarding Detection (BFD) with OSPF. BFD is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and, if a timer runs out on a connection, that router is declared to be down. BFD then communicates this information to OSPF, and the routing information is updated.

For additional information about OSPF routing, see the OSPF section of the FortiOS Handbook.

Terminology

Link State: Information is shared between directly connected routers. This information propagates throughout the network unchanged and is also used to create a shortest path first (SPF) tree.

Autonomous System (AS) : A network under a common network administration.

Area: You can divide a large network into areas to limit the number of link-state updates.

Cost: The routing metric used by OSPF. Lower costs are always preferred. You can configure the cost or use the interface default.

Router ID: Each OSPF router requires a unique router ID. For FortiSwitch, the unique router ID must be assigned manually.

Adjacency: When two OSPF routers have exchanged information and have the same topology table.

Topology Table: Also called the link-state table. This table contains information about every link in the network. The SPF algorithm uses the link-state information to calculate the best route to each destination.

Designated Router (DR): This router is responsible for ensuring adjacencies between all neighbors on a multi-access network (such as Ethernet). This ensures all routers do not need to maintain full adjacencies with each other. The DR is selected based on the router priority. In a tie, the router with the highest router ID is selected.

Backup DR: A backup router designed to perform the same functions in case the DR fails.

Link-State Advertisement (LSA): The method used by each router to share its routing topology with other routers in the same area.

Area Border Router (ABR): Router located on the border of one or more OSPF areas that connects those areas to the backbone area.

AS Boundary Router (AS BR): ABR located between an OSPF autonomous system and a non-OSPF network.

How OSPF Works

Areas

An OSPF implementation consists of one or more areas. An area consists of a group of contiguous networks. If you configure more than one area, Area Zero is always the backbone area. An ABR links one or more areas to the OSPF backbone area.

FortiSwitch supports different types of areas—stub areas, Not So Stubby areas (NSSA), and regular areas. A stub area is an interface without a default route configured. NSSA is a type of stub area that can import AS external routes and send them to the backbone but cannot receive AS external routes from the backbone or other areas. All other areas are considered regular areas.

Adjacencies

When an OSPF router boots up, it sends OSPF Hello packets to find neighbors on the same network. Neighbors exchange information, and the Link State databases of both neighbors are synchronized. At this point, these neighbors are said to be adjacent.

For two OSPF routers to become neighbors, the following conditions must be met:

- The subnet number and subnet mask for the interface must match in both routers.
- The Hello interval and Dead interval values must match.
- The routers must have the same OSPF area ID.
- If authentication is used, they must pass authentication checks.

In OSPF, routing protocol packets are only passed between adjacent routers.

FortiSwitch OSPF Capabilities

FortiSwitch supports the following capabilities:

- Support for OSPFv2.
- OSPF neighbors support authentication
- Supports NSSA
- Supports BFD
- Supports stub area
- Network scaling

NOTE: OSPF MIBs are not supported in this release.

Configuring OSPF

Using the web-based manager:

1. Create a switched virtual interface. See "Layer 3 Interfaces" on page 115.
2. Go to **Router > Router > OSPF**.
3. Enter a unique 32-bit number in dotted decimal format for the router identifier. **NOTE:** Without a router identifier, OSPF routing will not work.
4. Select an area and click **Create New**.
   - Select if the area is a stub area, NSSA, or a regular area.
   - If you want routing authentication, select **MD5** or **Text**.
   - Click **OK**.
5. Under **Networks**, click **Create New**.
   - Enter the IP address and netmask, separated with a space. Use an IP address that includes the switched virtual interface.
   - Select the area that you created.
   - Click **OK**.
6. Under **Interfaces**, click **Create New**.
   - Enter a descriptive name for the OSPF interface name.
   - Select the switched virtual interface that you created.
   - Select the same type of authentication that you selected for the area.
   - If you want static bidirectional forwarding detection, select **Enable** or **Global**.
   - Enter the maximum transmission unit.
   - Enter the cost.
   - Enter the number of seconds between Hello packets being sent.
   - Enter the number of seconds that a Hello packet is not received before the OSPF router decides that a neighbor has failed.
   - Click **OK**.
7. Click **Advanced Options (BFD, Default Route, Redistribution)**.
   - If you are going to advertise non-OSPF routes within OSPF, enter the metric (cost) for other routing protocols.
   - Click **Apply**.

Using the CLI:

Configuring OSPF on FortiSwitch includes the following major steps:

1. **config router ospf** - Enter OSPF configuration mode.
2. **set router-id** - Each router must have a unique 32-bit number. **NOTE:** Without a router identifier, OSPF routing will not work.
3. **config area** - You must create at least one area.
4. **config network** - Attach one or more networks to each area.
5. **config ospf-interface** - Configure an interface to a peer OSPF router.
6. **config redistribute** - Advertise these non-OSPF routes within OSPF.

1. config router ospf

Enter OSPF configuration mode to access all of the OSPF configuration commands:

```
# config router ospf
```

2. set router-id

Each router within an area must have a unique 32-bit number. The router-id is written in dotted decimal format, but it is not an IPv4 address. **NOTE:** Without a router identifier, OSPF routing will not work.

```
set router-id <router-id>
```

Example:

```
# config router ospf
(ospf) # set router-id 1.1.1.2
```

3. config area

You must create at least one area. The area number is written in dotted decimal format (for example, configure area 100 as 0.0.0.100).

```
config area
   edit <area number>
      set authentication {md5 | none | text}
      set shortcut (default | disable | enable)
      set type {nssa | regular | stub}
end
```

Example:

```
(ospf) # config area
(area) # edit 0.0.0.4
(0.0.0.4) # set type nssa
(0.0.0.4) # set authentication md5
```

4. config network

Use this subcommand to identify the OSPF-enabled interfaces. The prefix length in the interface must be equal or larger than the prefix length in the network statement.

```
config network
   edit <network number>
      set area <area>
      set prefix <network prefix> <mask>
```

Example:

```
(ospf) # config network
(network) # edit 1
(1) # set area 0.0.0.4
(1) # set prefix 10.1.1.0 255.255.255.0
```

5. config ospf-interface

Configure interface-related OSPF settings. Enter a descriptive name for the OSPF interface name. Use **set interface** to apply this configuration to a FortiSwitch interface:

```
config ospf-interface
   edit <ospf interface name>
      set interface <interface name>
      set priority <>
```

Example:

```
(ospf) # config ospf-interface
(ospf-interface) # edit oi1
(oi1) # set interface vlan40-p4
(oi1) # set priority 255
```

Note: The following values must match for an adjacency to form:

- area type and number
- interface subnet and mask
- hello interval
- dead interval

6. config redistribute

Redistribute non-OSPF routes (directly connected or static routes) within OSPF:

```
config redistribute { <name> | connected | rip | static }
   set status enable
   set metric <integer>
   set metric-type {1 | 2}
end
```

Example:

```
(ospf) # config redistribute connected
(connected) # set status enable
```

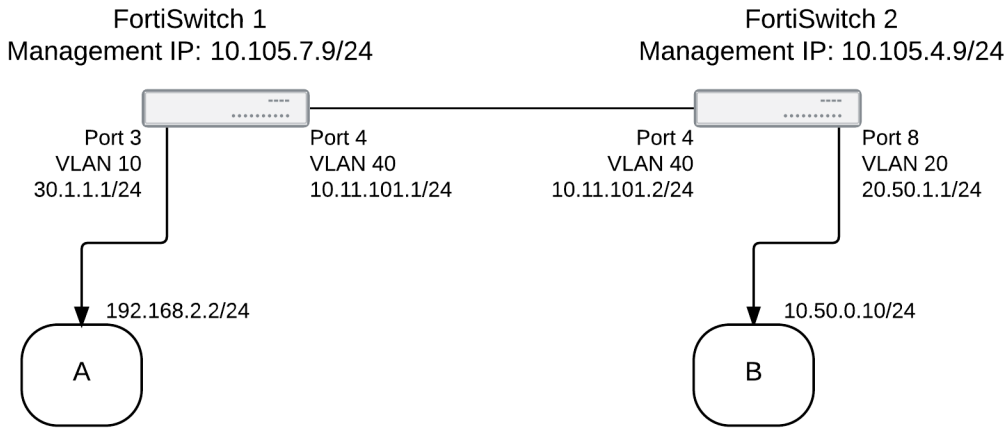
Display Commands

The **get router info ospf** command has options to display different aspects of the OSPF configuration and status. For example:

```
get router info ospf neighbors
get router info ospf database
```

Example Configuration

The following example shows a very simple OSPF network with one area. FortiSwitch1 has one OSPF interface to FortiSwitch 2:



Configure System Interfaces (Same Configuration Steps as for Static Routing)

Switch 1

```
config system interface
   edit vlan10-p3
      set ip 30.1.1.1 255.255.255.0
      set allowaccess ping https http ssh telnet
      set vlanid 10
   next
   edit vlan40-p4
      set ip 10.11.101.1 255.255.255.0
      set allowaccess ping https http ssh telnet
      set vlanid 40
end
config switch interface
   edit "port3"
      set native-vlan 10
   next
   edit "port4"
      set native-vlan 40
   next
end
```

Switch 2

```
config system interface
   edit vlan20-p8
```

```
      set ip 20.50.1.1 255.255.255.0
      set allowaccess ping https http ssh telnet
      set vlanid 20
   next
   edit vlan40-p4
      set ip 10.11.101.2 255.255.255.0
      set allowaccess ping https http ssh telnet
      set vlanid 40
end
config switch interface
   edit "port8"
      set native-vlan 20
   next
   edit "port4"
      set native-vlan 40
   next
end
```

Configure OSPF Router

Configure OSPF with the following:

1. Set the router ID.
2. Create the area.
3. Create the network (set network prefix and associate with an area).
4. Configure the OSPF interface.
5. Redistribute the routes.

Switch 1

```
config router ospf

   set router-id 10.11.101.1

   config area
      edit 0.0.0.0
      next
   end

   config network
      edit 1
         set area 0.0.0.0
         set prefix 10.11.101.0 255.255.255.0
      next
   end

   config ospf-interface
      edit "1"
         set cost 100
         set interface "vlan10"
         set priority 100
      next
   end
```

```
   config redistribute connected
      set status enable
   end

end
```

Switch 2

```
config router ospf
   set router-id 10.11.101.2

   config area
      edit 0.0.0.0
      next
   end

   config network
      edit 1
         set area 0.0.0.0
         set prefix 10.11.101.0 255.255.255.0
      next
   end

   config ospf-interface
      edit "1"
         set cost 100
         set interface "vlan10"
         set priority 100
      next
   end

   config redistribute connected
      set status enable
   end

end
```

Verify OSPF Neighbor

```
get router info ospf neighbor all
```

Verify the Routes Are Exchanged Using OSPF

```
get router info ospf route
```

RIP Routing

NOTE: You must have an advanced features license to use RIP routing.

The Routing Information Protocol (RIP) is a distance-vector routing protocol that works best in small networks that have no more than 15 hops. Each router maintains a routing table by sending out its routing updates and by asking neighbors for their routes. RIP is relatively simple to configure on FortiSwitch units but slow to respond to network outages. RIP is better than static routing but less scalable than Open Shortest Path First (OSPF).

FortiSwitch supports RIP version 1 and RIP version 2:

- RIP version 1 uses classful addressing and broadcasting to send out updates to router neighbors. It does not support different sized subnets or Classless Inter-Domain Routing (CIDR) addressing.
- RIP version 2 supports classless routing and subnets of various sizes. Router authentication supports MD5 and authentication keys. Version 2 uses multicasting to reduce network traffic.

RIP uses three timers:

- The update timer determines the interval between routing updates. The default setting is 30 seconds.
- The timeout timer is the maximum time that a route is considered reachable while no updates are received for the route. The default setting is 180 seconds. The timeout timer setting should be at least three times longer than the update timer setting.
- The garbage timer is the is the how long that the FortiSwitch advertises a route as being unreachable before deleting the route from the routing table. The default setting is 120 seconds.

You can enable Bidirectional Forwarding Detection (BFD) with RIP. BFD is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and, if a timer runs out on a connection, that router is declared to be down. BFD then communicates this information to RIP, and the routing information is updated.

For additional information about RIP routing, see the Routing Information Protocol (RIP) section of the FortiOS Handbook.

Terminology

Access list: A list of IP addresses and the action to take for each one. Access lists provide basic route and network filtering.

Active RIP interface: Each RIP router sends and receives updates by actively communicating with its neighbors.

Keychain: A list of one or more authentication keys including its lifetime, which is how long each key is valid.

Metric: RIP uses hop count as the metric for choosing the best route. A hop count of 1 represents a network that is connected directly to the FortiSwitch. A hop count of 16 represents a network that cannot be reached.

Passive RIP interface: The RIP router listens to updates from other routers but does not send out updates. A passive RIP interface reduces network traffic.

Prefix list: A more powerful prefix-based filtering mechanism. A prefix is an IP address and netmask.

Split horizon: A way to avoid routing loops.

Configuring RIP

NOTE: You must create a keychain first before you can use the MD5 authentication mode with RIP version 2. To add a new keychain using the CLI:

```
config router key-chain
   edit <keychain identifier>
   next
end
```

Using the web-based manager:

1. Create a switched virtual interface (SVI). See "Layer 3 Interfaces" on page 115.
2. Go to **Router > Router > RIP**.
3. Select whether you want to use RIP version 1 or RIP version 2 and click **Apply**. RIP version 2 is the default.
4. If you have a complex configuration, select the appropriate options under **Advanced Options**.
5. Enter an IP address and netmask for your RIP network, separated with a slash, and click **Add**. For example, 172.168.200.0/255.255.255.0. **NOTE:** Select an IP address for a network that includes all SVIs that you want to use. You can configure multiple network ranges to cover all SVIs that will be using RIP routing.
6. To enable interface-specific features (such as authentication and the RIP version to send and receive routing updates), select the appropriate options under **Interfaces**.

Using the CLI:

```
config router rip
   config network
      edit <network identifier>
         set prefix <network prefix> <mask>
      next
   end
end
```

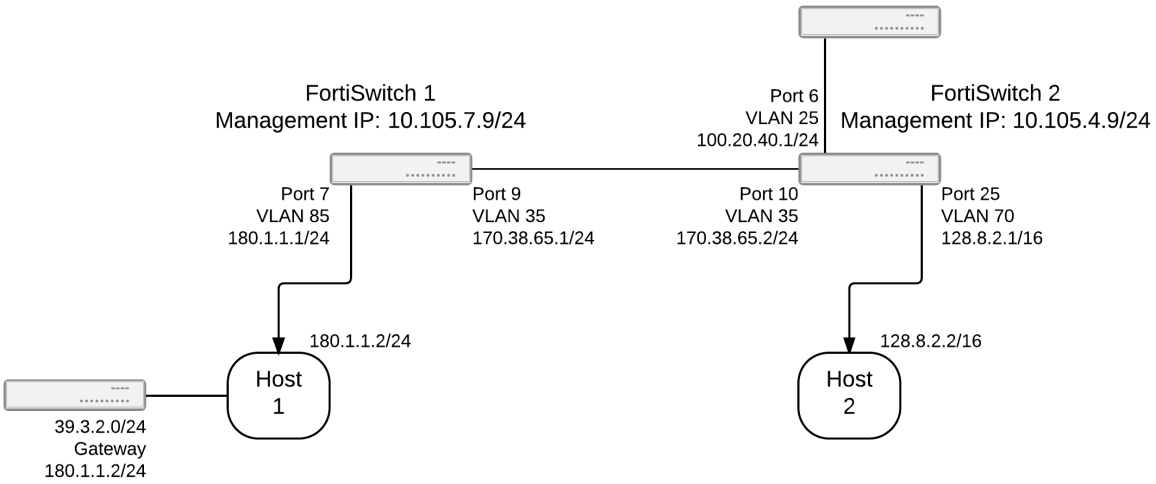
Display commands

The **get router info rip** command has options to display different aspects of the RIP configuration and status. For example, there are options to display the RIP general information and the RIP database:

```
get router info rip status
get router info rip database
```

Example Configuration

The following example shows a very simple RIP network:



Switch 1: Configure the Switch Interface

```
config switch interface
   edit "port9"
      set allowed-vlans 35
   next
   edit "port7"
      set allowed-vlans 85
   next
end
```

Switch 1: Configure the System Interface

```
config system interface
   edit "vlan35"
      set ip 170.38.65.1/24
      set allowaccess ping https http ssh snmp telnet
      set vlanid 35
   next
   edit "vlan85"
      set ip 180.1.1.1/24
      set allowaccess ping https http ssh snmp telnet
      set vlanid 85
   next
end
```

Switch 1: Configure the RIP Router; Add Authentication Between FortiSwitch 1 and FortiSwitch 2

```
config router rip
   config network
```

```
      edit 1
         set prefix 170.38.65.0/24
      next
      edit 2
         set prefix 180.1.1.0/24
      next
   end
   config interface
      edit "vlan35"
         set auth-mode text
         set auth-string simplepw1
      next
   end
end
```

Switch 1: Add a Static Route and Redistribute It

```
config router static
   edit 1
      set dst 39.3.2.0 255.255.255.0
      set gateway 180.1.1.2
   next
end

config router rip
   config redistribute "static"
      set status enable
   next
end
```

Switch 2: Configure the Switch Interface

```
config switch interface
   edit "port10"
      set allowed-vlans 35
   next
   edit "port25"
      set allowed-vlans 70
   next
end
```

Switch 2: Configure the System Interface

```
config system interface
   edit "vlan35"
      set ip 170.38.65.2/24
      set allowaccess ping https http ssh snmp telnet
      set vlanid 35
   next
   edit "vlan70"
      set ip 128.8.2.1/16
      set allowaccess ping https http ssh snmp telnet
      set vlanid 70
   next
end
```

Switch 2: Configure the RIP Router; Add Authentication Between FortiSwitch 1 and FortiSwitch 2

```
config router rip
   config network
      edit 1
         set prefix 170.38.65.0/24
      next
      edit 2
         set prefix 127.8.0.0/16
      next
   end
   config interface
      edit "vlan35"
         set auth-mode text
         set auth-string simplepw1
      next
   end
end
```

Switch 2: Add a Connected Route and Redistribute It

```
config switch interface
   edit "port6"
      set allowed-vlans 25
   next
end
config system interface
   edit "vlan25"
      set ip 100.20.40.1/24
      set allowaccess ping https http ssh snmp telnet
      set vlanid 25
   next
end

config router rip
   config redistribute "connected"
      set status enable
   next
end
```

VRRP Routing

NOTE: You must have an advanced features license to use VRRP.

The Virtual Router Redundancy Protocol (VRRP) uses virtual routers to control which physical routers are assigned to an access network. A VRRP group consists of a master router and one or more backup routers that share a virtual IP address. If the master router fails, the VRRP automatically assigns one of the backup routers without affecting network traffic. When the failed router is functioning again, it becomes the master router again. VRRP provides this redundancy without user intervention or additional configuration to any of the devices on the network.

To create a VRRP group, you need to create a VRRP virtual MAC address, which is a shared MAC address adopted by the VRRP master. The VRRP virtual MAC address feature is disabled by default. You must enable the VRRP virtual MAC address feature on all members of a VRRP group.

The VRRP master router sends VRRP advertisement messages to the backup routers. When the VRRP master router fails to send advertisement messages, the backup router with the highest priority takes over as the master router.

For additional information about VRRP, see the VRRP section of the FortiOS Handbook.

Configuring VRRP

Using the web-based manager:

1. Go to **System > Network > Interface**.
2. Select an interface and click **Edit**.
3. (Optional) Select the **VRRP Virtual MAC** check box.
4. Click **Add** to add a virtual router.
5. Enter the unique virtual router identifier.
6. Enter the VRRP group number.
7. Enter the priority. If the highest priority value of 255 is entered, the virtual router becomes the master router.
8. Select the **Preempt** check box if you want the router to preempt the master virtual router if the priority changes.
9. Enter the virtual IP address that will be shared across the VRRP group.
10. Enter one or two IP addresses that the master router must track. The maximum number of IP addresses is two. If these IP addresses cannot be reached by the master router, the priority of the master router changes to 0.
11. Click **OK**.
12. Click **Add** to add each additional virtual router.
13. After filling in the fields for each additional virtual router, click **OK**.

Using the CLI:

```
config system interface
   edit <VLAN name>
      set ip <IP address> <netmask>
      set allowaccess <access_types>
```

```
      set vrrp-virtual-mac enable
         config vrrp
            edit <VRRP router identifier>
               set priority <priority number>
               set vrgrp <VRRP group number>
               set vrip <virtual IP address>
            next
         end
      set snmp-index <index number>
      set vlanid <VLAN identifier>
      set interface "internal"
   next
end
```

Example of configuring VRRP:

```
config system interface
   edit "vlan-8"
      set ip 10.10.10.1 255.255.255.0
      set allowaccess ping https http ssh
      set vrrp-virtual-mac enable
         config vrrp
            edit 5
               set priority 255
               set vrgrp 50
               set vrip 11.1.1.100
            next
            edit 6
               set priority 200
               set vrgrp 50
               set vrip 11.1.1.100
            next
            edit 7
               set priority 150
               set vrgrp 50
               set vrip 11.1.1.100
            next
         end
      set snmp-index 20
      set vlanid 8
      set interface "internal"
   next
end
```

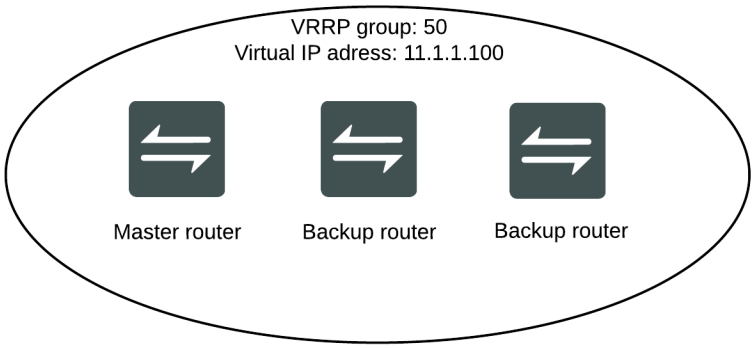
Display command

Use the **get router info vrrp** command to display the VRRP status:

```
get router info vrrp
```

Example Configuration

The following example shows a VRRP group with one master router and two backup routers:



Users and User Groups

FortiSwitch provides authentication mechanisms to control user access to the system (based on the user group associated with the user). The members of user groups are user accounts. Local users and peer users are defined on the FortiSwitch. User accounts can also be defined on remote authentication servers.

This section describes how to configure local users and peer users and how to configure user groups. For information about configuring the authentication servers, see Remote Authentication Servers.

Users

A user account consists of a user name, password, and potentially other information, configured in a local user database or on an external authentication server.

Users can access resources that require authentication only if they are members of an allowed user group.

Local and remote users are defined in **System** > **User** > **User Definition**.

```
config user local
   edit <username>
      set ldap-server <servername>
      set passwd <password_str>
      set radius-server <servername>
      set tacacs+-server <servername>
      set status {enable | disable}
      set type <auth-type>
   end
```

Field	Description
username	Identifies the user
passwd	A password for the local user
ldap-server <servername>	To authenticate this user using a password stored on a remote authentication server, select the type of server and then select the server from the list. You can select only a server that has already been added to the FortiSwitch configuration.
radius-server <servername>	
tacacs+-server <servername>	
status	Enable or disable this user.

User Groups

A user group contains a list of local and remote users.

Security policies allow access to specified user groups only. This restricted access enforces Role Based Access Control (RBAC) to your organization's network and its resources. Users must be in a group and that group must be part of the security policy.

```
config user group
   edit <groupname>
      set authtimeout <timeout>
      set group-type <grp_type>
      set http-digest-realm <attribute>
      set member <names>
      config match
         edit <match_id>
            set group-name <gname_str>
            set server-name <srvname_str>
      end
   end
```

The table below describes the parameters

Field	Description
groupname	Identifies the user group.
authtimeout <timeout>	Sets the authentication timeout for the user group. The range is 1 to 480 minutes. If this field is set to 0, the global authentication timeout value is used.
group-type <grp_type>	Enter the group type. <grp_type> determines the type of users and is one of the following: **firewall** - FortiSwitch users defined in user local, user ldap or user radius **fsso-service** - Directory Service users
http-digest-realm <attribute>	Enter the realm attribute for MD5-digest authentication.
member <names>	Enter the names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Separate the names with spaces. To add or remove names from the group, you must re-enter the whole list with the additions or deletions required.
config match fields	
<match_id>	Enter an ID for the entry.

Field	Description
group-name <gname_str>	Identifies the matching group on the remote authentication server.
server-name <srvname_str>	Specifies the remote authentication server.

802.1x Authentication

To control network access, FortiSwitch supports IEEE 802.1x authentication. A supplicant connected to a port on the switch must be authenticated by a RADIUS/Diameter server to gain access to the network. The supplicant and the authentication server communicate using the switch using EAP protocol.

To use the RADIUS server for authentication, you must configure the server before configuring the users or user groups on the FortiSwitch.

FortiSwitch implements MAC-based authentication. The switch saves the MAC address of each supplicant's device. The switch provides network access only to devices that have successfully been authenticated.

You can enable the MAC Authentication Bypass (MAB) option for devices (such as network printers) that cannot respond to the 802.1x authentication request. With MAB enabled on the port, the system will use the device MAC address as the username and password for authentication.

Optionally, you can configure a guest VLAN for unauthorized users. Alternatively, you can specify a VLAN for users whose authentication was unsuccessful.

Dynamic VLAN assignment

You can configure the RADIUS server to return a VLAN in the authentication reply message.

To assign a VLAN dynamically to the port, use the following commands:

```
config switch interface
   edit <interface_name>
      set security-mode 802.1X
```

The FortiSwitch will change the native VLAN of the port to that of the VLAN from the server.

To assign a VLAN dynamically to an authenticated user on a port, use the following commands:

```
config switch interface
   edit <interface_name>
      set security-mode 802.1X-mac-based
```

Here, the switch assigns the returned VLAN only to this user's MAC address. The native VLAN of the port remains unchanged.

Use the following configuration command to view the MAC-based VLAN assignments:

```
diagnose switch vlan assignment mac list [sorted-by-mac | sorted-by-vlan]
```

Configure the following attributes in the RADIUS server:

- Tunnel-Private-Group-Id - 10 (vlanid)
- Tunnel-Medium-Type - IEEE-802(6)
- Tunnel-Type - VLAN (13)

MAC Authentication Bypass (MAB)

NOTE: The following SKUs do not support MAB: FS-108D-POE, FS-224D-POE, and FSR-112D-POE.

Devices such as network printers, cameras, and sensors might not support 802.1x authentication. If you enable the MAB option on the port, the system will use the device MAC address as the username and password for authentication.

You must provision the RADIUS server to authenticate the devices that use MAB, either by adding the MAC addresses as regular users or by implementing additional logic to resolve the MAC addresses in a network inventory database.

Configuring Global Settings

Use the following commands to configure the global settings:

```
config switch global
   config port-security
      set reauth-period <0-1440>
      set max-reauth-attempt <0-15>
      set link-down-auth {no-action | set-unauth}
```

NOTE: Changes to global settings only take effect when new 802.1x/MAB sessions are created.

Variable	Description
reauth-period	This setting defines how often the device needs to reauthenticate (that is, if a session remains active beyond this number of minutes, the system requires the device to reauthenticate). The default value is 60 minutes. Set the value to 0 to disable reauthentication.
max-reauth-attempt	If 802.1x authentication fails, this setting caps the number of reattempts that the system will initiate. The range is from 0 to 15 where "0" translates to forever (fail causes a log message). The default value is 3.
link-down-auth	If a link goes down, this setting determines whether the impacted devices must reauthenticate. Set the value to **no-action** if reauthenication is unecessary. Set the value to **set-unauth** to revert all devices to the un-authenticated state. Each device must reauthenticate.The default is **set-unauth**.

Configuring the Interface

Use the following commands to configure the 802.1x settings on an interface:

```
config switch interface
   edit <port>
      config port-security
         set port-security-mode {none | 802.1X}
```

```
set mac-auth-bypass {enable | disable}
set guest-vlan {enable | disable}
set guest-vlanid <vlanid>
set guest-auth-delay <integer>
set auth-fail-vlan {enable | disable}
set auth-fail-vlanid <vlanid>
set radius-timeout-overwrite {enable | disable}
```

Variable	Description
port-security-mode	Set security mode. None (no security) is the default.
mac-auth-bypass	Enable the feature. Default is disable.
guest-vlan and auth-fail-vlan	The system assigns the **guest-vlan** to unauthorized users. After the system assigns the **auth-fail-vlan** to users who attempted to authenticate but failed to provide valid credentials. If you enable either **guest-vlan** or **auth-fail-vlan**, you must configure the corresponding VLAN ID (otherwise, the configuration save attempt will fail when you enter **next** or **end**).
guest-auth-delay	Time when an authorization fails after the guest is applied. In seconds ranging from 60 to 900. Default is 120.
radius-timeout-overwrite	This setting specifies whether to use the RADIUS-provided re-authentication timeout. If the setting is enabled, the port uses the local timeout (see Configuring Global Settings). If the setting is disabled, the system uses the value of the RADIUS Access-Accept message Session-Timeout attribute to determine the duration of the session. It uses the Termination-Action value to determine the device action when the session's timer expires. If the Termination-Action attribute is present and its value is RADIUS-Request, the device port re-authenticates the host. If the Termination-Action attribute is not present, or its value is Default, the device port terminates the session. If the device port is configured to use the RADIUS-supplied timeout, but the Access-Accept message does not include a Session-Timeout attribute, the device port never re-authenticates the supplicant.

Other Commands

Use the following command to manually flush all authorizations on a given port:

```
execute 802-1x clear interface <port>
```

Use the following command to show diagnostics on one or all ports:

```
diagnose switch 802-1x status [<port>]
```

```
port3 : Mode: port-based (MAC by-pass disable)
Link: Link up
Port State: authorized
Dynamic Authorized Vlan: 10
Native vlan: 10
Allowed vlan list: 1-10
Untagged vlan list:
Guest vlan:
AuthFail vlan:

Sessions info:
STA=00:24:9b:1b:20:65 Type=802.1X EAP PEAP state=AUTHENTICATED

port4 : Mode: mac-based (MAC by-pass enable)
Link: Link up
Port State: authorized
Native vlan: 10
Allowed vlan list: 10,11
Untagged vlan list:
Guest vlan: 503
AuthFail vlan: 603

Authorized Client MAC TYPE VLAN Dynamic-VLan
00:24:9b:1b:20:65 802.1X 11 11
00:24:9b:1b:1f:11 MAB 10

Sessions info:
STA=00:24:9b:1b:20:65 Type=802.1X,PEAP state=AUTHENTICATED params:reauth=90
STA=00:24:9b:1b:1f:11 Type=MAB state=AUTHENTICATED params:reauth=120
```

Access Profile Override

Optionally, you can configure the RADIUS server to set the access profile. This process uses RADIUS vendor-specific attributes (VSAs) passed to the FortiSwitch for authorization.

In the following example, we create a RADIUS-system admin group with accprofile-override enabled:

```
config system admin
   edit "RADIUS_Admins"
      set remote-auth enable
      set accprofile no_access
      set wildcard enable
      set remote-group "RADIUS_Admins"
      set accprofile-override enable
```

```
    next
```

Ensure that the RADIUS server is configured to send the appropriate VSA.

To send an appropriate group membership and access profile, we must set VSA 1 and VSA 6, as in the following:

```
VENDOR fortinet 12356
ATTRIBUTE Fortinet-Group-Name 1 <admin profile>
ATTRIBUTE Fortinet-Access-Profile 6 <access profile>
```

The value of VSA 1 must match the remote group, and VSA 6 must match a valid access profile.

Authenticating Users with a RADIUS server

Using the CLI:

1. Create a RADIUS user group:

```
config user radius
   edit <name>
      set server <address>
   end
end
```

2. Create a user group:

```
config user group
   edit <name>
      set member <list>
      config match
         edit 1
            set group-name <name>
            set server-name <name>
         end
      end
   end
end
```

3. Configure the switch interface for port-based 802.1x:

```
config switch interface
   edit <interface>
      set security-mode 802.1X
      set security-groups <name>
   end
end
```

4. Configure the switch interface for MAC-based 802.1x:

```
config switch interface
   edit <interface>
      set security-mode 802.1X-mac-based
      set security-groups <name>
   end
end
```

Using the web-based manager:

NOTE: Define the RADIUS server and remote user group using the CLI (steps 1 and 2 above):

1. Go to **Switch > Interface > Interface** and select the port to update.
2. Set **Security Mode** to either **802.1x** or **802.1x-mac-based.**
3. Select **OK.**

Example: RADIUS user group

Here, we configure a RADIUS user group and show the associated CLI syntax:

1. Create a RADIUS user:

```
config user radius
   edit "FortiAuthenticator"
      set secret ENC
          6rF7O4/Zf3p2TutNyeSjPbQc73QrS21wNDmNXd/rg9k6nTR6yMhBRsJGpArhle6UOCb7b8InM3n
          rCeuVETr/a02LpILmIltBq5sUMCNqbR6zp2fS3r35Eyd3IIrzmve4Vusi52c1MrCqVhzzy2Efxk
          Brx5FhcRQWxStvnVt4+dzLYbHZ
      set server "10.160.36.190"
   next
end
```

2. Create a user group:

```
config user group
   edit "Radius_group"
      set member "FortiAuthenticator"
   end
end
```

3. Configure a port:

```
config switch interface
   edit "port1"
      set allowed-vlans 1
      set security-mode 802.1X
      set security-groups "Radius_group"
      set snmp-index 1
   end
end
```

Example: Dynamic VLAN

To assign VLAN dynamically for a port on which a user is authenicated, configure the RADIUS server attributes to return the VLAN ID when the user is authenticated. Assuming that the port security mode is set to 802.1X, the FortiSwitch will change the native VLAN of the port to the value returned by the server.

Ensure that the following attributes are configured on the RADIUS server:

- Tunnel-Private-Group-Id <integer> (the VLAN ID)
- Tunnel-Medium-Type IEEE-802 (6)

- Tunnel-Type VLAN (13)

Authenticating an Admin User with RADIUS

If you want to use a RADIUS server to authenticate administrators, you must configure the authentication before you create the administrator accounts. Do the following:

- Configure the FortiSwitch to access the RADIUS server.
- Configure an administrator to authenticate with a RADIUS server and match the user secret to the RADIUS server entry.
- Create the RADIUS user group.

Using the CLI:

1. Create a RADIUS system admin group:

```
config system admin
   edit "RADIUS_Admins"
      set remote-auth enable
      set accprofile "super_admin"
      set wildcard enable
      set remote-group "RADIUS_Admins"
   next
end
```

2. Create a user:

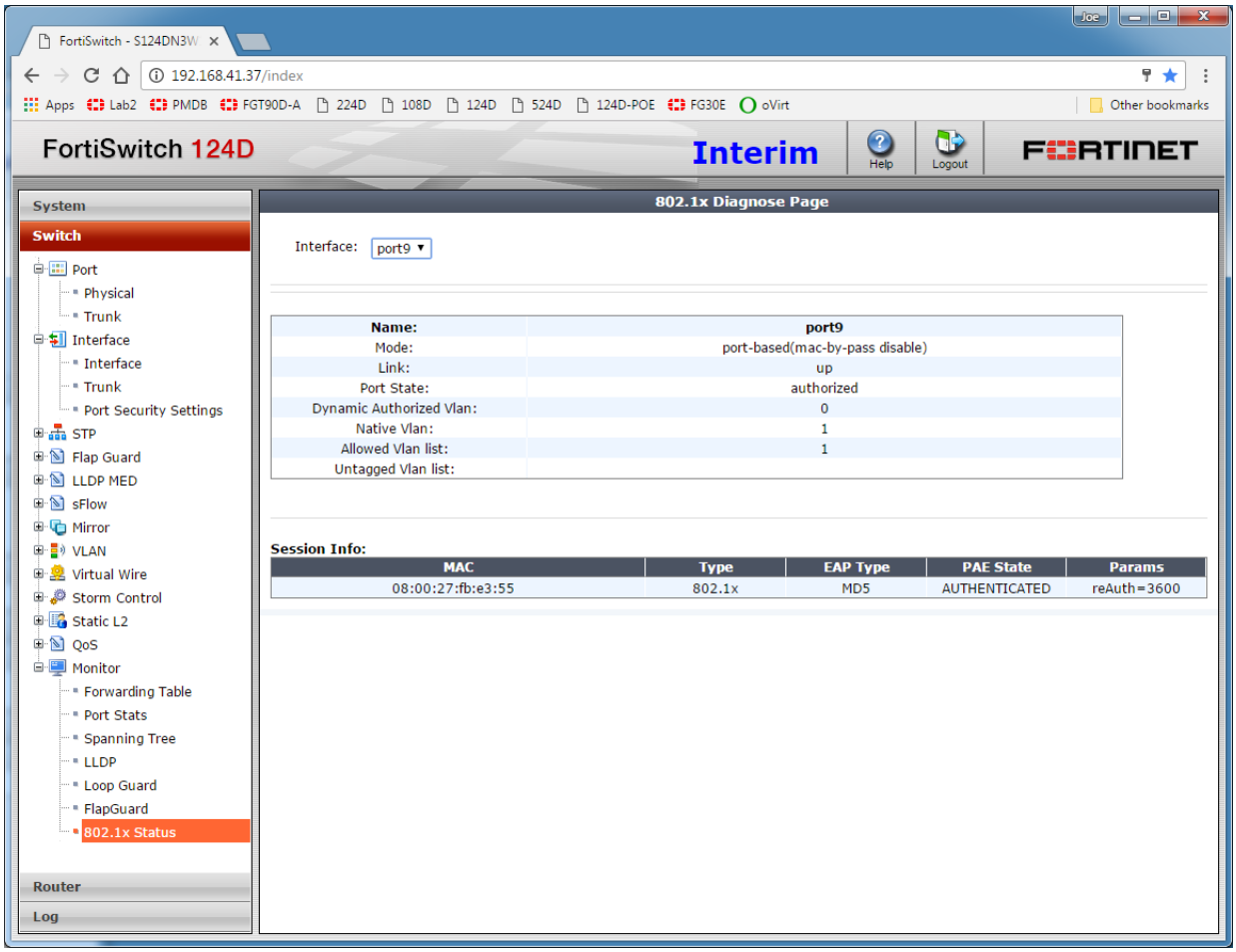
```
config user radius
   edit "RADIUS1"
      set secret
   next
end
```

3. Create a user group:

```
config user group
   edit "RADIUS_Admins"
      set member "RADIUS1"
   next
end
```

GUI Display of dot.1x Details

Select **System>Switch>Monitor>802.1x Status**:


FortiSwitch - S124DN3W
192.168.41.37/index
Apps Lab2 PMDB FGT90D-A 224D 108D 124D 524D 124D-POE FG30E oVirt Other bookmarks
FortiSwitch 124D
Interim
Help
Logout
FORTINET
System
Switch
Port
Physical
Trunk
Interface
Interface
Trunk
Port Security Settings
STP
Flap Guard
LLDP MED
sFlow
Mirror
VLAN
Virtual Wire
Storm Control
Static L2
QoS
Monitor
Forwarding Table
Port Stats
Spanning Tree
LLDP
Loop Guard
FlapGuard
802.1x Status
Router
Log
802.1x Diagnose Page
Interface: port9
Name: port9
Mode: port-based(mac-by-pass disable)
Link: up
Port State: authorized
Dynamic Authorized Vlan: 0
Native Vlan: 1
Allowed Vlan list: 1
Untagged Vlan list:
Session Info:
MAC Type EAP Type PAE State Params
08:00:27:fb:e3:55 802.1x MD5 AUTHENTICATED reAuth=3600

TACACS

This chapter contains information on using TACACS authentication with your FortiSwitch unit, describing the following tasks:

- Configuring the FortiSwitch to access the TACACS+ server
- Creating a TACACS+ user group
- Configuring an administrator to authenticate with a TACACS+ server

Administrative Accounts

Administrative, or admin, accounts allow access to various aspects of the FortiSwitch configuration. The level of access is determined by the admin profile that is assigned to the admin account.

See Configuring Admin Tasks for the steps to create an admin profile.

Configuring a TACACS Admin Account

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices using one or more centralized servers. If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiSwitch contacts the TACACS+ server for authentication.

Using the web-based manager:

1. Go to **System > Admin > Administrators** and select **Create New**.
2. Give the administrator account an appropriate name.
3. Set **Type** as **Remote.**
4. Set **User Group** to a group for remote users.
5. Enable **Wildcard**.
6. Set **Admin Profile** to use the new profile.
7. Select **OK**.

Using the CLI:

```
config system admin
   edit tacuser
      set remote-auth enable
      set wildcard enable
      set remote-group <group>
      set accprofile <profile>
   end
end
```

User Accounts

User accounts identify a network user and determine what parts of the network the user is allowed to access.

Configuring a User Account

```
config user tacacs+
   edit <tacserver>
      set authen-type {ascii | auto | chap | ms_chap | pap}
      set authorization enable
      set key <authorization_key>
      set server <server>
   end
end
```

Configuring a User Group

```
config user group
   edit <tacgroup>
      set member <tacserver>
      config match
         edit 1
            set server-name <server>
            set group-name <group>
         end
      end
   end
end
```

Example Configuration

The following is an example configuration of a TACACS user account, with the CLI syntax shown to create it:

1. Configuring a TACACS user account for login authentication:

```
config user tacacs+
   edit tacserver
   set authen-type ascii
   set authorization enable
   set key temporary
   set server tacacs_server
end
```

2. Configuring a TACACS user group:

```
config user group
   edit tacgroup
      set member tacserver
      config match
         edit 1
            set server-name tacserver
            set group-name tacgroup
         end
```

```
      end
   end
end
```

3. Configuring a TACACs system admin user account:

```
config system admin
   edit tacuser
      set remote-auth enable
      set wildcard enable
      set remote-group tacgroup
      set accprofile noaccess
   end
end
```

Troubleshooting and Support

This chapter covers tips and best practices for troubleshooting and support.

Virtual Wire

Some testing scenarios may require two ports to be wired 'back-to-back'. Instead of using a physical cable, you can configure a virtual wire between two ports. The virtual wire forwards traffic from one port to the other port with minimal filtering or modification of the packets.

Notes:

- ACL mirroring is not supported.
- You can select ports that are already ingress and egress mirror sources.

Using the web-based manager:

1. Go to **Switch > Virtual Wire > Wire**.
2. Click **Create New** to create a new virtual wire.
3. Enter a name and select the ports for first member and second member.
4. Click **OK** to save the changes.

Using the CLI:

Use the following commands to configure a virtual wire:

```
config switch virtual-wire
   edit <virtual-wire-name>
      set first-member <port-name>
      set second-member <port-name>
      set vlan <vlan-id>
   next
end
```

Virtual wire ports set a special Tag Protocol Identifier (TPID) in the VLAN header. The default value is **0xdee5**, a value that real network traffic never uses.

Use the following commands to configure a value for the TPID:

```
config switch global
   set virtual-wire-tpid <hex value from 0x0001 to 0xFFFE>
end
```

Use the following command to display the virtual wire configuration:

```
diagnose switch physical-ports virtual-wire list
  port1(1) to port2(2) TPID: 0xdee5 VLAN: 4011
  port3(3) to port4(4) TPID: 0xdee5 VLAN: 4011
  port5(5) to port25(25) TPID: 0xdee5 VLAN: 4011
  port7(7) to port8(8) TPID: 0xdee5 VLAN: 4011
```

Note the following information about virtual wire:

- Ports have ingress and egress VLAN filtering disabled. All traffic (including VLAN headers) is passed unchanged to the peer. All egress traffic is untagged.
- Ports have L2 learning disabled.
- Ports have their egress limited to their peer and do no allow egress from any other ports.
- The system uses TCAM to force forwarding from a port to its peer.
- The TCAM prevents any copy-to-cpu or packet drops.

TFTP Network Port

When you power on the FortiSwitch, the BIOS performs basic device initialization. When this activity is complete, and before the OS starts to boot, you can click any key to bring up the boot menu.

From the menu, click the "I" key to configure TFTP settings. With newer versions of the BIOS, you can specify the network port (where you have connected your network cable). If you are not prompted to specify the network port, you must connect your network cable to the default network port:

- If the switch model has a WAN port, the WAN port is the network port.
- If the switch has no WAN port, the highest port number is the network port.

Set the Boot Partition

You can specify the flash partition for the next reboot. The system can use the boot image from either the primary or the secondary flash partition:

```
execute set-next-reboot <primary|secondary>
```

If your FortiSwitch model has dual flash memory, you can use the primary and backup partitions for image rotation. By default, this feature is disabled.

```
config system global
   set image-rotation <enable | disable>
end
```

To list all of the flash partitions:

```
diagnose sys flash list
```

Cable Diagnostics

You can check the state of cables connected to a specific port. The following pair states are supported:

- Open
- Short
- Ok
- Open_Short

- Unknown
- Crosstalk

If no cable is connected to the specific port, the state is Open, and the cable length is 0 meters.

For supported models, see "Introduction" on page 10.

Using the web-based manager:

1. Go to **Switch > Port > Physical**.
2. Select a port.
3. Click **Cable Diag**.
4. Click **Ok** to start the cable diagnostics. **NOTE**: Cable diagnostics will temporarily disable the link on the port, which interrupts network traffic.
5. Click **OK** to close the Cable Diagnostics window.

Using the CLI:

Use the following command to run a time domain reflectometry (TDR) diagnostic test on cables connected to a specific port:

```
diagnose switch physical-ports cable-diag <physical port name>
```

For example:

```
# diagnose switch physical-ports cable-diag port1

port1: cable (4 pairs, length +/- 10 meters)
pair A Open, length 0 meters
pair B Open, length 0 meters
pair C Open, length 0 meters
pair D Open, length 0 meters
```

Use the following command to check the medium dependent interface crossover (MDI-X) interface status for a specific port:

```
diagnose switch physical-ports mdix-status <physical port name>
```

For example:

```
# diagnose switch physical-ports mdix-status port1

port1: MDIX(Crossover)
```

Selective Packet Sampling

NOTE: This feature is not supported on 3032.

During debugging, you might want to see whether a particular type of packet was received on an interface on the switch.

1. Set up an access control list (ACL) on the switch with the interface that you want to monitor. See "Access Control Lists " on page 86. This ACL is the ingress interface.
2. Set up a mirror for the “internal” interface.

For example, if you want to monitor interface port17 for any IP packet (ether-type 0x800) with a destination subnet of 10.10.10/24 and a source subnet of 20.20.20/24, use the following commands.

```
# show switch acl policy
config switch acl policy
   edit 1
      config action
         set mirror "internal"
      end
      config classifier
         set dst-ip-prefix 10.10.10.0 255.255.255.0
         set ether-type 0x0800
         set src-ip-prefix 20.20.20.0 255.255.255.0
      end
      set ingress-interface "port17"
   next
end
```

To examine the packets that have been sampled in the example, use the following command:

```
# diagnose sniffer packet sp17 none 6
```

Deployment Scenario

Working Configuration for PC and Phone for 802.1x Authentication Using MAC

Summary

A. Configure all devices.
   - PC
   - Phone
   - FortiSwitch
   - FortiAuthenticator
   - DHCP server

B. Authenticate phone using MAB and using lldp-med.

C. Authenticate PC using EAP 802.1x.

A. Configure All Devices

1. Configure the PC, phone, FortiSwitch, FortiAuthenticator [RADIUS server], and DHCP server).

Phone Configuration (file: macmode_phone_pc_ping_work)

1. On the phone, enable the WAN port and leave the VLAN ID at the default to allow LLDP-Med (Policy) designate for voice VLAN assignment.
2. On the phone, enable the LAN port and assign the VLAN ID for data matching the RADIUS VLAN assignment.

PC Configuration

1. Install the supplicant software.
2. Launch the supplicant software, key in username/password, and enable DHCP on the interface.

FortiSwitch Configuration

1. Configure lldl profile for voice.

```
# show switch lldp
config switch lldp profile

edit "pexa" <<<<<<<<<<<<<<<<<
   set 802.1-tlvs port-vlan-id
      config med-network-policy
         edit "voice"
            set status enable
```

```
            set vlan 21
        next
        edit "voice-signaling"
            set status enable
            set vlan 31
        next
        edit "guest-voice"
        next
        edit "quest-voice-signaling"
        next
        edit "softphone-voice"
            set status enable
            set vlan 41
        next
        edit "video-conferencing"
        next
        edit "streaming-video"
        next
        edit "video-signaling"
        next
    end
set med-tlvs inventory-management network-policy
```

2. Apply lldl profile on a dot1x port.

```
# show switch physical-port port4
config switch physical-port

    edit "pexa" <<<<<<<<<<<<<<<<
    set lldp-profile "pexa"
    set speed auto
    next
end
```

3. Configure a user group.

```
# show user group
config user group

    edit "Corp_Grp_10"
    set member "FAC_LAB"
    next
end
```

4. Configure the RADIUS server.

```
# show user radius
config user radius

    edit "FAC_LAB" <<<<<<<<<
    set secret

    ENCW82jBg06XhKD/4Dugqm8QF2f7D1B4bfFdDSZaLUQPwZXv4F8zMc5sWHRl9suwmbmzNnAnyqPaa
        rAYcSLuT8kVjFSRO0znx+TXVWTqdSeLCpbMv
        +HYFNOHMbYlfES8wTYYD40InCgrYr2johvr2vfa5KG4g8XMwKSIM0LurR//1WqT0fH
    set server
    next
```

```
end
```

5. Configure port security on the dot1x port.

   a. Configure mac-mode port-security.
   b. Add voice VLAN on allowed list (for example, 21).
   c. Apply the security group.

   Interface port4 configuration:

```
# show switch interface port4
config switch interface

   edit "port4"
   set allowed-vlans 20-21,31,41
   set security-groups "Corp_Grp_10"
   set snmp-index 4
configure port-security
   set auth-fail-vlan disable
   set guest-auth-delay 120
   set guest-vlan disable
   set mac-auth-bypass enable
   set port-security-mode 802.1X-mac-based
   set radius-timeout-overwrite disable
   set auth-fail-vlanid 40
   set guest-vlanid 30
end
```

RADIUS Configuration

MAB Authentication:

1. Add phone MAC address to MAB list.

802.1X Authentication

1. Create a local user.
2. Create a user group with "Attributes" and enable PEAP and MSChapv2.

DHCP Configuration

1. On the DHCP server, configure a pool for phone and a pool for the PC.

```
!
ip dhcp pool PC
network 10.1.1.0 255.255.255.0
default-router 10.1.1.1
dns-server 10.1.1.1
!
ip dhcp pool PC
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
dns-server 20.1.1.5
```

2. Configure exclude lists for pools for both gateway and DNS.

```
ip dhcp excluded-address 20.1.1.1 20.1.1.1.5
```

```
<<<<gateway and dns server
ip dhcp excluded-address 10.1.1.1 10.1.1.1.5
<<<<gateway and dns server
!
ip dhcp pool PC
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
dns-server 20.1.1.5
```

3. Configure the switch port VLAN interface as a gatweway for the phone.

```
# show run
Building configuration

Current configuration
!
interface vlan21 <<<<<<
ip address 20.1.1.1
end
```

4. Configure the switch port VLAN interface as a gatweway for the PC.

```
# show run
Building configuration

Current configuration
!
interface vlan10 <<<<<<
ip address 10.1.1.1
end

#
```

5. Configure the l2 port and associate the voice VLAN.

```
# show run
Building configuration

Current configuration
!
interface GigabitEthernet g1/0/1 <<<<<<
switchport access vlan 21
switchport trunk encapsulation dot1q
switchport trunk all
switchport mode trunk
end
```

6. Configure the l2 port and associate the data VLAN.

```
# show run
Building configuration

Current configuration
!
interface GigabitEthernet g1/0/2 <<<<<<
switchport access vlan 10
```

```
switchport trunk encapsulation dot1q
switchport trunk all
switchport mode trunk
end
```

2. Connect a link between the FortiSwitch and the DHCP server and assign matching VLAN for the phone for both ports.

3. Connect a link between the FortiSwitch and the DHCP server and assign a matching VLAN for the PC for both ports.

B. Authenticate Phone Using MAB

1. Connect the phone to the switch to authenticate with RADIUS through the MAB (mac-bypass).
2. Once authenticated:
   a. On the FortiSwitch, verify that the port is authorized and that the voice VLAN is on the allowed list.

```
# diagnose switch 8 status
Signal 10 received - config reload scheduled

wrdapd_hostapd_dump_state_console Hostapd own address 90:6c:ac:18:6f:2f
dump_diag:1:
receive dump diagnostic 802_1x/MAB sessions. ifname :port4: dump_diag:1:

port4 : Mode: mac-based (mac-by-pass enable)
        Link: Link up
        Port State: authorized ( ) <<<<<<
        Native Vlan : 1
        Allowed Vlan list: 1,10,20-21,31,41 <<<<<<
        Untagged Vlan list:
        Guest VLAN:

        Client MAC Type Vlan Dynamic-Vlan
        68:f7:28:fb:c0:0f 802.1x 1 10
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<phone

        Sessions info:
        68:f7:28:fb:c0:0f Type=802.1x,PEAP,state=AUTHENTICATED
        params:reAuth=3600
        00:a8:59:d8:f1:f6 Type=MAB,,state=AUTHENTICATED
        params: reAuth=3600

        edited on: 2016-11-29 17:25

        edited on: 2016-11-29 17:59
```

   b. On the FortiSwitch, verify that the lldp neighbor detail accurately reflects the phone and voice VLAN designation.

```
        Neighbor learned on port4 by LLDP protocol
Last change 140 seconds ago
Last packet received 13 seconds ago

Chassis ID: 20.1.1.10 (ip) <<<<<<<<<<
System Name: FON-670i
```

```
System Description
V12.740.335.12.B

Time To Live: 60 seconds
System Capabilities: BT
Enabled Capabilities: BT
MED type: Communication Device Endpoint (Class III)
MED Capabilities: CP
Management IP Address: 20.1.1.10

Port ID: 00:a8:59:d8:f1:f6 (mac) <<<<<<<<<<<<<<<
Port description: WAN Port 10M/100M/1000M
IEEE802.3, Power via MDI:
Power devicetype: PD
PSE MDI Power: Not Supported
PSE MDI Power Enabled: No
PSE Pair Selection: Can not be controlled
PSE power pairs: Signal
Power class: 1
Power type: 802.3at off
Power source: Unknown
Power priority: Unknown
Power requested: 0
Power allocated: 0
LLDP-MED, Network Policies:
voice: VLAN: 21 (tagged), Priority: 0 DSCP: 0 <<<<<<<<<<<<
voice-signaling: VLAN: 21 (tagged), Priority: 0 DSCP: 0
streaming-video: VLAN: 21 (tagged), Priority: 0 DSCP: 0

# Checking STA 00:a8:59:d8:f1:f6 inactivity:
Station has been active
```

c. On the phone, verify that the DHCP address is assigned.

d. On the DHCP server, check binding and ping from gateway to verify that the phone is reachable.

```
# show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
20.1.1.10 00a8.59d8.f1f6 Mar 20 1993 01:52 AM Automatic
#
#
#
# show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
10.1.1.7 0168.f728.fbc0.0f Mar 11 1993 01:54 AM Automatic <<<<<< pc
20.1.1.10 00a8.59d8.f1f6 Mar 20 1993 01:52 AM Automatic <<<<< phone
# ping 10.1.1.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.7, timeout is 2
!!!!!
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
# ping 10.1.1.7
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
# ping 10.1.1.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
# ping 20.1.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
#
```

C. Authenticate the PC Using EAP dot1x

1. Connect the PC to the phone for EAP authentication and VLAN assignment (for data)
2. Once authenticated:
   a. On the FortiSwitch, verify that the port is authorized and that the data VLAN assigned to dynamic has been placed on the allowed list.

```
# diagnose switch 8 status
Signal 10 received - config reload scheduled

wrdapd_hostapd_dump_state_console Hostapd own address 90:6c:ac:18:6f:2f
dump_diag:1:
receive dump diagnostic 802_1x/MAB sessions. ifname :port4: dump_diag:1:

port4 : Mode: mac-based (mac-by-pass enable)
        Link: Link up
        Port State: authorized ( ) <<<<<<
        Native Vlan : 1
        Allowed Vlan list: 1,10,20-21,31,41
   <<<<<<
        Untagged Vlan list:
        Guest VLAN:

        Client MAC Type Vlan Dynamic-Vlan
        68:f7:28:fb:c0:0f 802.1x 1 10
<<<<<<<<<<<<<<<<<<<<<<< PC
        00:a8:59:d8:f1:f6 MAB 1 0

        Sessions info:
        68:f7:28:fb:c0:0f Type=802.1x,PEAP,state=AUTHENTICATED
        params:reAuth=3600
        00:a8:59:d8:f1:f6 Type=MAB,,state=AUTHENTICATED

        params:reAuth=3600

        edited on: 2016-11-29 17:25
```

```
edited on: 2016-11-29 17:59
```

b. On the PC, verify that the DHCP address is assigned.
c. From the DHCP server, check the binding and a ping from gateway to verify that the PC is reachable.